UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Titulo: Notificación Electrónica. Firma digital en la Administración pública.
Autores: Ignacio Raúl Machado
Director: Lic. Paula Venosa
Codirector: Lic. Nicolás Macia
Asesor profesional: Ing. Juan Enrique Coronel
Asesor profesional: Lic. Sebastián Pardo
Carrera: Licenciatura en Sistemas

Resumen

Se expone el trabajo realizado para la implementación de la solución del proyecto de Notificación electrónica en el Honorable Tribunal de Cuentas de la Provincia de Buenos Aires. Se describe el desarrollo de los componentes de dicho proyecto y cómo los mismos interactúan entre sí. Además se presenta uno de los componentes con mayor énfasis y detalle, Segno, el firmador digital. Esta herramienta además de firmar digitalmente documentos de tipo PDF, se integra en forma transparente con las aplicaciones web existentes del organismo. Dicho desarrollo aborda la extensa temática estudiando todos los conceptos que la involucran, analizando diferentes casos de éxito y explicando los procesos relacionados.

Palabras Claves

Firma Digital, Segno, Herramienta Informática, Honorable Tribunal de Cuentas, Provincia de Buenos Aires, Notificación Electrónica, Domicilio Electrónico

Trabajos Realizados

- Estudio del Proyecto de Notificación Electrónica.
- Diseño e implementación de la solución del proyecto de Notificación Electrónica.
- Análisis de firmadores digitales ya implementados.
- Implementación de Segno.

Conclusiones

La implementación del proyecto de Notificación electrónica permitió acelerar notablemente los tiempos de notificación hacia los controlados por el organismo. Cabe destacar, la importancia del desarrollo de Segno en el ámbito público donde el uso de firma digital se va incorporando lentamente en los procesos administrativos.
El desafío para los próximos años, será fomentar la utilización de la firma digital tanto en usuarios particulares como en organismos privados.

Trabajos Futuros

- Mejorar el mecanismo de interacción de Segno con los sistemas internos del Organismo.
- Desarrollar nuevas funcionalidades para que el usuario pueda personalizar su firma.
- Soporte para firmar otro tipo de documentos.

Fecha de la presentación: Septiembre de 2017

Agradecimientos

A mis padres Marita y Raúl, por haberme enseñado la importancia de no bajar los brazos y que todo esfuerzo da sus frutos.

A mis hermanos Nico y Fer, por estar siempre y acompañarme durante todos estos años.

A mi novia Estefanía por ser mi compañera de vida, apoyarme en cada proyecto que emprendo e impulsarme a seguir para adelante frente a las adversidades.

A mis amigos por estar siempre dispuestos a escuchar y dar la palabra justa.

A mis compañeros de trabajo por el soporte diario y brindarme el acceso a los recursos necesarios para el desarrollo de este trabajo.

A mis directores de tesina Paula y Nicolás por la paciencia y dedicación que me brindaron desde su lugar, atendiendo las dudas que fueron surgiendo.

A mis asesores profesionales Juan y Sebastián, por estar en el día a día y orientarme durante todo el transcurso de la tesina.

Índice general

Capítulo 1

1. Introducción

En los últimos años la tecnología se ha ido incorporando a las tareas de la vida cotidiana y a las organizaciones de todo tipo. No pueden negarse las ventajas que ha traído la inclusión de la misma en tareas que años atrás requerían mucho más tiempo y esfuerzo; por tales motivos los organismos gubernamentales la adoptaron rápidamente para la recepción de solicitudes, generación de documentación, pagos mediante sistemas web y múltiples actividades.
Puntualmente en la Administración Pública se han logrado diversos avances, teniendo en cuenta la necesidad de priorizar aspectos como la celeridad y la minimización de los costos. El proceso de notificación no ha sido la excepción y por lo tanto se ha promovido la modernización de forma clara y concreta a través de la firma de leyes y decretos.
En Diciembre de 2001 se sancionó la Ley Nacional 25.506[1] que establece la validez jurídica para la firma digital.
Este paso inició un camino hacia la modernización del estado, utilizando recursos ya existentes que requieren un ejercicio de la función administrativa eficiente incorporando instrumentos que posibiliten una progresiva utilización de las nuevas tecnologías de la información y comunicaciones.
En el año 2007 la provincia de Buenos Aires se adhirió a la normativa impulsada por Nación por medio de la ley 13.666 [2]. Asimismo, el Honorable Tribunal de cuentas de la Provincia de Buenos Aires (HTC) [3] mediante la resolución 7/2015 [4] formalizó la creación del proyecto “Notificación Electrónica”.
Estas medidas, entre otras, dan cuenta que tanto a nivel nacional como provincial, el estado se ha involucrado en la modernización de los procesos y ha actuado en consecuencia respecto a condiciones legales y tecnológicas en pos de mejorar las actividades desarrolladas dentro de la administración pública.
En búsqueda de agilizar y mejorar notablemente una de las tareas más importantes dentro del organismo, se logró dar comienzo al proyecto anteriormente mencionado

1.1. Objetivos

- Estudiar y analizar la notificación electrónica en el ámbito de la Administración Pública Provincial.
- Diseñar la solución para el proyecto de “Notificación Electrónica” a implementarse en el Honorable Tribunal de Cuentas de la Provincia de Buenos Aires
- Desarrollar un firmador digital aplicable en el HTC, siendo factible su implementación en cualquier organismo público o privado.

1.2. Motivación

La notificación electrónica surge como una alternativa inmediata para lograr que los procesos judiciales se desarrollen con mayor celeridad, economía y seguridad procesal.
EL HTC se encuentra comprometido en un proceso de mejora continua , con el objetivo de obtener agilidad, eficacia y eficiencia en las tareas que se realizan diariamente. Por lo tanto, resulta de vital importancia la incorporación y utilización de las nuevas tecnologías de la información y las comunicaciones.
En este contexto se gestó la idea del proyecto de Notificación Electrónica, contemplando el desarrollo del firmador digital *"Segno"*. Esta herramienta nace ante la necesidad de firmar digitalmente documentos PDF generados dentro del HTC de acuerdo a la Ley Nacional de Firma Digital con el objetivo de hacer más eficiente su gestión y disminuir los tiempos de respuesta.

1.3. Estructura organizativa

La presente tesina de grado contiene 6 Capítulos, los cuales contienen las etapas de investigación del proyecto de notificación electrónica y desarrollo del firmador digital Segno utilizado en el HTC.

Inicialmente, en el capítulo 2 se hace una introducción a la criptografía, abordando los diferentes criptosistemas que existen, haciendo énfasis en RSA, utilizado para la firma de documentos. Además se explican los conceptos fundamentales relacionados con firma digital.

En el capítulo 3 se describen los conceptos fundamentales de la notificación como proceso legal, los antecedentes de la notificación electrónica en organismos públicos y su abordaje dentro del gobierno electrónico.

El capítulo 4 contiene el diseño de solución del proceso de Notificación electrónica dentro del Honorable Tribunal de Cuentas de la Provincia de Buenos Aires.

En el capítulo 5 se presenta el firmador digital implementado, Segno, describiendo el proceso de desarrollo y sus funcionalidades.

Por último en el capítulo 6 se especifican las conclusiones finales del presente trabajo, así como también los trabajos proyectados a futuro.

Capítulo 2

2. Introducción a la Criptografía

2.1.Conceptos básicos

La criptografía[5] es tan antigua como la escritura y permite, gracias a la aplicación de técnicas, cifrar información de cierta manera que observadores no autorizados no puedan acceder a la misma.
Existe una amplia variedad de disciplinas donde se aplica, entre las que se destaca la Teoría de la Información, la complejidad algorítmica, la teoría de números o matemática discreta, entre otras.
Actualmente la criptografía es un pilar fundamental para la seguridad de la información, por lo que tiene gran relevancia en cuestiones que involucran firma digital.
A lo largo de este capítulo se verán las funciones que cumple la criptografía, los métodos de cifrado simétrico y asimétrico.
Finalmente se hace hincapié sobre el método RSA utilizado para la firma digital.

2.1.1. La criptografía y sus funciones en la seguridad de información

La criptografía se utiliza, entre otras aplicaciones, para garantizar el cumplimiento de ciertas propiedades en una comunicación y brindar seguridad mediante su empleo:

- **Confidencialidad**: La información es accedida solamente por observadores autorizados consolidando exclusividad en sus lecturas.

- **Integridad**: La información no sufre ningún cambio en el proceso de cifrado/descifrado por lo que se dice que correcta y completa. Para lograrlo se utilizan distintas herramientas como funciones MDC[6], protocolos de compromiso de bits[7] o protocolos de rabin[8].

- **No repudio**: Mediante diferentes mecanismos se puede asociar un documento a una persona o a un sistema criptográfico. De esta manera dicha información queda vinculada a un individuo particular, sin la posibilidad de poder negar haber participado.También, en otro contexto, puede ser necesario negar la intervención de un individuo (para ello se utilizan técnicas como el cifrado negable[9]).

- **Autenticidad del autor**: Provee mecanismos que permiten verificar la identidad del autor del documento. Para lograrlo se pueden usar , por ejemplo, funciones de hash[10]

2.1.2. Sistemas de cifrado

Un sistema de cifrado se define formalmente como una quintupla (M, C, K, E, D), donde:

- M es el conjunto de mensajes no cifrados listos para ser enviados.
- C hace referencia a todos los mensajes cifrados.
- K representa el conjunto de claves que pueden ser utilizadas.
- E representa al conjunto de funciones que se aplican a cada elemento de M para obtener un elemento de C. Hay tantas transformaciones Ek posibles como número de claves(K) definidas.
- D es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

$$D_k(E_k(m)) = m$$

Es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obteniendo finalmente de nuevo el mensaje.

2.1.3. Tipos de criptosistemas

Existen dos tipos básicos de criptosistemas o sistemas de cifrado:

- **Criptosistemas simétricos o de clave privada**: Son aquellos que emplean una misma clave **k** tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar en posesión tanto en el emisor como en el receptor, lo cual obliga a realizar la distribución de claves a través de un medio seguro.

- **Criptosistemas asimétricos o de clave pública**, éstos emplean una doble clave (**kp,kP**). **kp** la cual se conoce como clave privada y **kP** como clave pública.

Puntualmente los criptosistemas de clave pública son los más adecuados en el proceso de firma digital. Los mismos, como se mencionó anteriormente utilizan doble clave (kp y kP).

Una de ellas sirve para la transformación de cifrado y la otra para la transformación de descifrado.

En muchos casos son intercambiables, es decir, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp.

Ofrecen una gran variedad de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros puesto que únicamente se envía por el canal la clave pública, que sólo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada (que no se puede obtener a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado.

En la práctica suele aplicarse una combinación de ambos sistemas de cifrados, ya que el criptosistema asimétrico posee la desventaja de necesitar mayor potencia de cómputo para cifrar y descifrar que los criptosistemas asimétricos.

Generalmente se hace uso de la criptografía asimétrica para codificar las claves simétricas y así enviarlas a los participantes en la comunicación, incluso a través de canales inseguros.

Después se codificarán los mensajes (más largos) intercambiados en la comunicación mediante algoritmos simétricos, que suelen ser más eficientes.

2.1.4. Criptosistema RSA

Como ya se ha mencionado, los criptosistemas de clave pública (también llamados *criptosistemas asimétricos*) se caracterizan por utilizar diferentes claves para el cifrado y descifrado de la información.

Su principal ventaja es que facilitan el proceso de distribución e intercambio de claves entre los participantes de la comunicación segura, lo cual era un problema importante de los criptosistemas simétricos o de clave privada.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos, que usan una única clave secreta. Por ejemplo, mientras que para segundos mencionados se considera segura una clave de 128 bits, para la mayoría de los primeros (incluido el del RSA [11]), se recomiendan actualmente claves de al menos 1024 bits de longitud. Además, la complejidad de cálculo que comportan los algoritmos de los criptosistemas asimétricos los hace considerablemente más lentos que los de cifrado simétricos. Por lo tanto en la práctica los métodos asimétricos se emplean principalmente para codificar la clave de sesión (simétrica) de cada comunicación o transacción particular.

Actualmente, el criptosistema de clave pública más importante y extendido en uso, es el **RSA**, que cifra y descifra por exponenciación modular, basando su seguridad en la complejidad del problema de la factorización de enteros grandes.

Entre todos los algoritmos asimétricos, RSA también quizás es el más sencillo de entender e implementar. Una peculiaridad de este algoritmo es que sus dos claves sirven indistintamente tanto para cifrar como para autenticar.

Debe su nombre a sus tres inventores: Ronald **Rivest**, Adi **Shamir** y Leonard **Adleman**, que publicaron por primera vez el método RSA en 1977. Ha estado bajo patente de los Laboratorios RSA hasta el 20 de septiembre de 2000, por lo que su uso comercial estuvo restringido hasta esa fecha.

RSA, como ya se ha indicado, se basa en la dificultad que presenta la factorización de números grandes. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos primos grandes. Un atacante que quiera recuperar un texto claro a partir del criptograma y de la clave pública, tiene que enfrentarse a dicho problema de factorización.

A continuación de describe cómo trabaja el algoritmo RSA:

- **Generación del par de claves**

Para generar un par de claves (KP ; Kp), en primer lugar se eligen aleatoriamente dos números primos grandes, *p* y *q* (de unas 200 cifras cada uno, por ejemplo). Después se calcula el producto $n = p.q$.

Escogeremos ahora un número *e* primo relativo con (*p*-1) y con (*q*-1). Este par de números (*e*,*n*) pueden ser conocidos por cualquiera, y constituyen la llamada *clave pública*

e por tanto debe tener un inverso módulo (*p*-1)(*q*-1), al que llamamos *d*. Por supuesto se cumple que $ed \equiv 1 \bmod((p-1)(q-1))$, equivaliendo $ed = 1+k(p-1)(q-1)$ para algún entero *k*.

La *clave privada* será el par (*d*,*n*). Este número *d* debe mantenerse secreto y sólo será conocido por el propietario del par de claves.

- **Cifrado del mensaje con la clave pública**

Cabe destacar que con este algoritmo los mensajes que se cifran y descifran son números enteros de tamaño menor que *n*, no letras sueltas como en el caso de los cifrados César o Vigènere.

Para obtener el mensaje cifrado *C* a partir del mensaje en claro *M*, se realiza la siguiente operación:

$$\mathbf{C = M^e \pmod n}$$

1. **Descifrado del mensaje con la clave privada**

Para recuperar el mensaje original a partir del cifrado se realiza la siguiente operación:

$$\mathbf{M = C^d \pmod n}$$

Justificación del método

$C^d \pmod{n} = (M^e)^d \pmod{n} = M^{1+k(p-1)(q-1)} \pmod{n} = (M^{(p-1)(q-1)})^k . M \pmod{n}$ [i]

Si recordamos, la función de Euler φ(n)= (p-1)(q-1), y que en general, salvo azar improbable, se tendrá que mcd(*M*,*p*)=mcd(*M*,*q*)=mcd(*M*,*n*)=1. Y por tanto según el teorema de Euler-Fermat, $M^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow (M^{(p-1)(q-1)})^k \equiv 1 \pmod{n}$ [ii]

De [i] y [ii] se obtiene que $C^d \pmod{n} = 1.M \pmod{n} = M$, para $0 \leq M < n$

- **Conmutatividad del cifrado y descifrado en RSA**

Por las propiedades de la exponenciación modular, el cifrado y descifrado son conmutativos:

$M = (M^e \bmod n)^d \bmod n = M^{d.e} \bmod n = (M^d \bmod n)^e \bmod n = M$

Esto supone que si cifrando M con la clave pública *e* y a continuación descifrando el resultado con la privada *d* obtenemos de nuevo M, también podemos cifrar M con la clave privada *d* y descifrar el resultado con la clave pública *e*, volviendo a obtener M.

Esta propiedad es importante porque nos permite utilizar RSA no sólo para cifrar un mensaje, sino también para **autenticar** el mensaje, como veremos en el tema siguiente.

- **Criptoanálisis del RSA**

Para romper un cifrado RSA, podemos probar varias vías. Aparte de factorizar *n*, que ya sabemos que es un problema computacionalmente intratable en un tiempo razonable, podríamos intentar calcular φ(n) directamente, o probar por un ataque de fuerza bruta tratando de encontrar la clave privada *d*, probando sistemáticamente con cada uno de los números posibles del espacio de claves. Ambos ataques son, para *n* grandes, incluso aún más costosos computacionalmente que la propia factorización de *n*.

2.1.5. El uso de RSA en la seguridad de la información

El criptosistema RSA no sólo permite garantizar la confidencialidad de la comunicación entre dos partes, cifrando en origen el mensaje que se va a transmitir por un canal inseguro y descifrandolo en recepción, sino que también proporciona otros servicios o funciones de seguridad de la información, como son la autenticación de origen y la integridad o el no-repudio (mediante la **firma digital**).
Para garantizar estos servicios suponiendo que existe una comunicación entre dos partes **A** y **B**, cada una de ellas generará antes de empezar su propio par de claves *(pública, privada)*. Así *A* tendrá el par (KP_A, kp_A) y *B* su par (KP_B, kp_B), donde **KP** son las claves públicas que son conocidas por las dos partes, y **kp** las privadas, que cada parte guarda la suya en secreto y no será conocida por la

otra parte. Recordar que $KP_A=(e_A,n_A)$ y $kp_A=(d_A,n_A)$. Lo mismo para el par de claves de *B*.

CIFRADO

Suponemos que *A* quiere enviar un mensaje *M* confidencialmente a *B* a través de un medio de transmisión inseguro. Estos son los pasos que tiene que seguir:

1. Obtiene la clave pública del destinatario *B*, (e_B,n_B)
2. Representa el texto en claro que quiere transmitir como un entero positivo M < n
3. Computa el mensaje cifrado: $C = (M)^e_B \bmod n_B$
4. Finalmente transmite el criptomensaje C por el canal inseguro

DESCIFRADO

Cuando *B* recibe el mensaje cifrado C, hace lo siguiente:

1. Usa su clave privada (d_B, n_B) para computar $M = (C)^d_B \bmod n_B$
2. Recupera el texto original a partir de su entero representante M

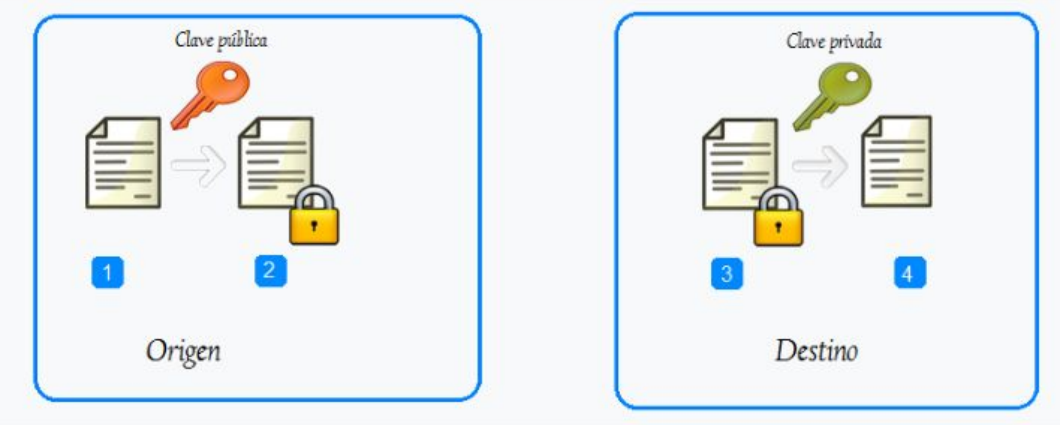


Fig.2.1. Cifrado asimétrico

2.2 Firma digital. Conceptos básicos

La firma digital[12] es un mecanismo tecnológico que permite garantizar la autoría e integridad de los documentos digitales, brindando las mismas características que posee un documento firmado tradicionalmente. La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que consolidan la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

2.2.1. Propiedades necesarias

Se han establecido las siguientes propiedades[13] que debe cumplir el esquema de firma digital para ser considerado legal:

- **Únicas:** las firmas deben poder ser generadas solamente por el firmante.

- **Infalsificables:** para falsificar una firma digital el atacante tiene que resolver problemas matemáticos de una complejidad muy elevada, es decir, las firmas han de ser computacionalmente seguras (por lo que la firma debe depender del mensaje en sí).

- **Verificables:** las firmas deben ser fácilmente verificables por los receptores de las mismas y, si es necesario, también por jueces o autoridades competentes.

- **Innegables:** el firmante no debe ser capaz de negar su propia firma.

- **Viables:** las firmas han de ser fáciles de generar por parte del firmante.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático al contenido, y a continuación aplicar un cifrado de tipo asimétrico o también llamado criptografía asimétrica (utilizando la clave privada del firmante) al resultado de la operación anterior.
Un esquema tradicional de firma digital consiste de tres algoritmos:

- Un algoritmo de generación de claves que selecciona la clave privada al azar de un conjunto de posibles claves privadas. El algoritmo devuelve la clave privada y su correspondiente clave pública.

- Un algoritmo de firmado, genera una firma , a partir de un mensaje y una clave privada. .

- Un algoritmo de verificación de firma, acepta o rechaza la autenticidad del mensaje, por medio de un mensaje, una clave pública y una firma.

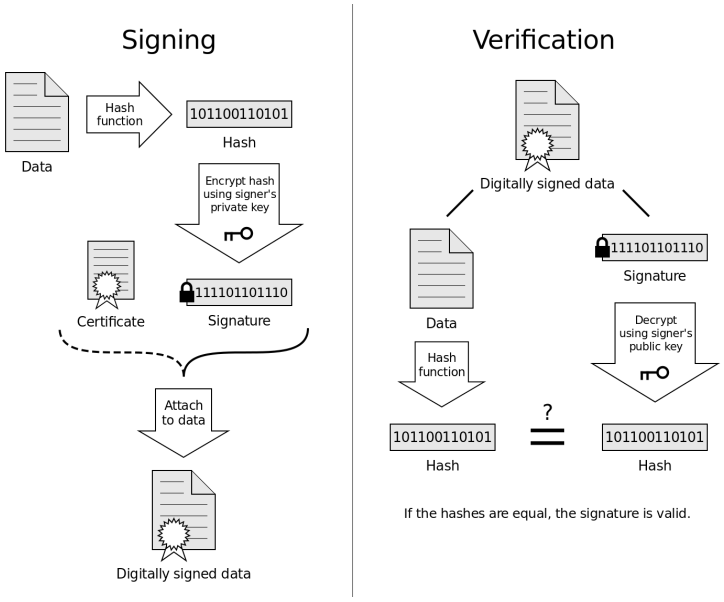


Fig.2.2. Esquema básico de firma digital

Dos propiedades principales son necesarias para el correcto funcionamiento de este esquema. En primer lugar, un firma generada desde un mensaje determinado y una clave privada debe verificar la autenticidad de dicho mensaje mediante la clave pública correspondiente.
Por otra parte, debe ser computacionalmente imposible generar una firma válida por alguién que no posea la clave privada.

La función *hash* es un algoritmo matemático que permite calcular un valor resumen de los datos firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. Sin embargo, este tipo de operaciones no fueron pensadas para que las lleve a cabo el usuario, sino que se utiliza un software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

2.2.2 Formatos de Firma electrónica

El formato de la firma[14] define cómo se genera el documento de firma y la forma en que se guarda la información en el documento de firma generado.
La existencia de múltiples formatos de firma electrónica se debe a razones históricas, de cómo se ha ido introduciendo ésta en documentos existentes y cómo se han ido añadiendo funcionalidades a lo largo del tiempo.
Un fichero de firma tiene un formato que se determina por diversos aspectos:

- **Estructura del fichero(** formatos CAdES, XAdES, PAdES, OOXML, ODF, etc).

- **Dónde se guarda el documento original**.

- **Firmas de múltiples personas.**

- **Longevidad de la firma y sellado digital en el tiempo.**

Las normas *TS 101 733[15]* y *TS 101 903* [16] definen los formatos técnicos de la firma electrónica. La primera se basa en el formato clásico PKCS7[17] y la segunda en XML-DSig[18], que consiste en la firma XML especificada por la W3C. Bajo estas normas se definen las tres modalidades de firma:

- **Firma básica:** Incluye el resultado de la operación de *hash* y clave privada, identificando los algoritmos utilizados y el certificado asociado a la clave privada del firmante.

- **Firma fechada:** A la firma básica se añade un sello de tiempo calculado a partir del *hash* del documento firmado por una TSA (Time Stamping Authority).

- **Firma validada o completa:** A la firma fechada se añade información sobre la validez del certificado procedente de una consulta de CRL o de OCSP realizada a la Autoridad de Certificación.

2.2.3. Infraestructura de clave pública (PKI)

En criptografía, una infraestructura de clave pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.
Esta tecnología permite a los usuarios autenticarse frente a otros usuarios y usar los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, entre otros usos.
En una operación criptográfica que use PKI, intervienen conceptualmente como mínimo las siguientes partes:

- Un usuario iniciador de la operación.

- Un conjunto de de autoridades que garantizan la validez de los certificados involucrados en la operación (Autoridad de Certificación, Autoridad de Registro y Sistema de sellado digital de tiempo).

- Un destinatario de los datos firmados por parte del usuario iniciador de la operación.

La seguridad que puede aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o Políticas de seguridad aplicados (como se ha detallado anteriormente, las operaciones criptográficas de clave pública, son procesos en los que se utilizan algoritmos de cifrado que son conocidos y están accesibles para todos).
La importancia de las políticas de seguridad en esta tecnología, es relevante , puesto que ni los dispositivos más seguros ni los algoritmos de cifrado más fuertes sirven si por ejemplo una copia de la clave privada protegida por una tarjeta criptográfica se guarda en un disco duro convencional de una PC conectada a Internet.

Componentes básicos de una PKI

A continuación se definen los componentes comunes a todos los modelos de infraestructura PKI.

- **PCA – POLICY CA's**

Para que un entorno de certificación funcione correctamente , es necesario definir una serie de reglas que indiquen la forma de aplicar los certificados.
Este conjunto de reglas que constituyen la Política de Certificación[19], tiene que estar definido por las autoridades reconocidas en el entorno. Por lo tanto, las CAs actuarán bajo una determinada política de certificación. Estas CA's específicas suelen denominarse PCA's (Policy CAs).
Una PCA puede estar representada por una empresa única, o una institución que agrupe a otras en representación, todo con el fin de definir el entorno, alcance y medios de las políticas de seguridad en la infraestructura.
Una política de seguridad establece y define la dirección de máximo nivel de una organización en base a la seguridad de información, así como los procesos y principios para el uso de la criptografía.
Por lo general, incluye declaraciones sobre cómo gestionará la empresa las Claves y la información crítica, y establecerá el nivel de control requerido para afrontar los niveles de riesgo.

- **CA – CERTIFICATION AUTHORITY**

Es una entidad o servicio que emite certificados. El sistema de CA es la base de confianza de una PKI, es uno de los pilares fundamentales de la infraestructura.
Como tal es un conjunto de herramientas y archivos asociados, que permiten comprobar la identidad de una persona, servidor o programa. Actuaría como una especie de notario electrónico.

Su función principal es el de avalar los datos de cualquier certificado emitido por la PKI.
Cada certificado emitido por una CA debe estar firmado por una CA de mayor grado en el esquema
jerárquico de autoridades certificadoras, formándose así una cadena de certificados, en los que unas CA se avalan a otras hasta llegar a la CA superior, que se avala a sí misma.
Esta jerarquía de firmas y la cadena con ella formada están contempladas en el estándar X.509 v3, que indica la forma correcta de realizar estas cadenas de certificaciones.
El Certificado Digital vincula pues indisolublemente a una persona o entidad con una llave pública, y mediante el sistema de firma digital se asegura que el certificado que recibimos es realmente de la persona que consta en el mismo.

- **RA – REGISTRATION AUTHORITIES**

Una RA, proporciona la interfaz entre el usuario y el CA. Captura y autentifica la identidad de los Usuarios y entrega la solicitud de certificado al CA. La calidad de este proceso de autentificación establece el nivel de confianza que puede otorgarse a los certificados.
Las RA's no realizan ninguna labor de certificación, su funcionalidad es la de registrar a las entidades o usuarios finales. Es decir, estas Autoridades se encargaran de garantizar que el binomio formado por una entidad y el par de claves que la identifica, sólo esté registrado una sola vez.
Las Autoridades de Registro estarán asociadas a las distintas Autoridades de Certificación que definen la jerarquía de un árbol, tanto a las Autoridades del nodo PCA, como a las CA's normales.
Aunque en algunos modelos las RA's son entidades lógicas separadas de las CAs, en la práctica pueden ser una misma entidad física, con un mismo DN (Distinguished Name). Es decir, una CA puede tener asociada y ubicada físicamente en el mismo sitio, a una RA que se encargue del registro de las entidades a las que certifica.
Para garantizar la validez del procedimiento de registro, cada RA deberá tener un par de claves asimétricas, con la clave pública certificada por una CA que sea un punto de confianza de todas las CA's para las que realiza funciones de registro. Cuando una RA y una CA coincidan físicamente, la RA podrá considerar el par de claves de la CA y su certificado como propios.

- **Repositorio**

Un entorno de Repositorio puede soportar el Directorio X.500, o almacenar los certificados en otro tipo de estructura. En aquellos entornos en los que se utiliza el Directorio X.500, el mecanismo de almacenamiento y obtención de certificados y CRL se simplifica.
Cada entidad de una infraestructura queda unívocamente identificada por su DN X.500 que indica cuál es su entrada en el Directorio. La recomendación X.500

define los atributos necesarios para almacenar la información relativa a certificación en el Directorio, de forma que cada entidad puede almacenar sus certificados en la correspondiente entrada. Si la entidad es una CA, además de sus certificados, en su entrada puede almacenar las CRL's asociadas.
Cuando una entidad necesita obtener un certificado de otra entidad o una CRL, una vez identificado el nombre de la otra entidad, puede localizar la información buscada en la entrada del Directorio de la otra entidad y la puede extraer, ya que estos atributos se configuran con permiso de lectura para todo el mundo. En el caso de utilización del Directorio como lugar de almacenamiento de certificados y CRL's es recomendable que el acceso al Directorio sea seguro.
Se puede utilizar un servidor de certificados y CRL's centralizado o distribuido, eso se definirá o mejor dicho estará definido por la PCA.

2.2.4. Certificados Digitales

Un certificado digital es un documento digital que permite identificar a una persona o una entidad de la misma manera que un pasaporte o licencia de conducir.
Un certificado digital es emitido por una autoridad, conocida como Autoridad Certificante (CA), la cual garantiza la validez de la información provista en el certificado.

Además, un certificado digital es válido sólo por un período de tiempo específico.
Los certificados digitales proporcionan soporte para la criptografía de clave pública porque los certificados digitales contienen la clave pública de la entidad identificada en el certificado. Dado que el certificado coincide con una clave pública para una persona en particular y la autenticidad del certificado está garantizada por el emisor, el certificado digital proporciona una solución al problema de cómo encontrar la clave pública de un usuario y sabe que es válida. Estos problemas son resueltos por un usuario que obtiene la clave pública de otro usuario del certificado digital. El usuario sabe que es válido porque una entidad de certificación de confianza ha emitido el certificado.
Además, los certificados digitales se basan en la criptografía de clave pública para su propia autenticación. Cuando se emite un certificado digital, la entidad emisora certificadora firma el certificado con su propia clave privada. Para validar la autenticidad de un certificado digital, un usuario puede obtener la clave pública de la entidad emisora de certificados y utilizarla contra el certificado para determinar si fue firmada por la entidad emisora de certificados.
Para que un certificado digital sea útil, tiene que ser estructurado de una manera comprensible y confiable para que la información dentro del certificado pueda ser recuperada y entendida fácilmente. Por ejemplo, los pasaportes siguen una estructura similar que permite a las personas entender fácilmente la información en un tipo de pasaporte que nunca han visto antes. De la misma manera, siempre y cuando los certificados digitales estén estandarizados, pueden ser leídos y entendidos independientemente de quién emitió el certificado.

El estándar S / MIME especifica que los certificados digitales utilizados para S / MIME cumplen con la norma X.509 de la Unión Internacional de Telecomunicaciones (ITU). S / MIME versión 3 requiere específicamente que los certificados digitales se ajusten a la versión 3 de X.509. Debido a que S / MIME se basa en un estándar establecido y reconocido para la estructura de certificados digitales, el estándar S / MIME se basa en el crecimiento de este estándar y, por lo tanto, aumenta su aceptación.
El estándar X.509 especifica que los certificados digitales contienen información estandarizada. En concreto, los certificados X.509 versión 3 contiene los siguientes campos:

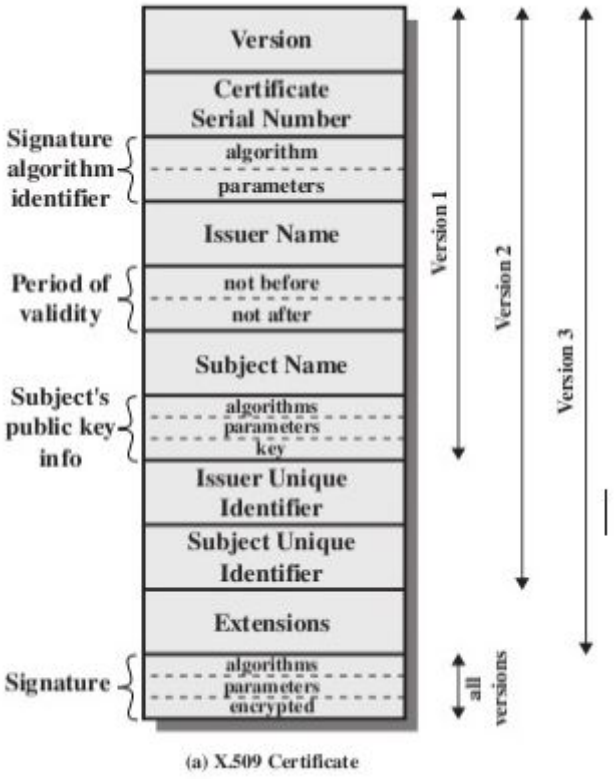


Fig. 2.3. Estructura de un certificado X.509

- **Version number:** Versión del estándar X.509, generalmente la 3, que es la más actual.
- **Serial number:** Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- **Certificate algorithm identifier:** Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- **Issuer name:** Este campo contiene información respecto a la Autoridad de Certificación que ha emitido el certificado digital, fundamentalmente del certificado de CA subordinada que se ha empleado para generar el certificado final.
- **Validity period:** Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información

sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.

- **Subject name:** Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- **Subject public key information:** Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- **Issuer unique identifier (opcional):** Este es un campo opcional que permite reutilizar nombres de emisor.
- **Subject unique identifier:** Estos campos contienen identificadores y aparecen en las versiones 2 o 3. Los identificadores del sujeto y del emisor son utilizados para la reutilización del nombre del emisor y el nombre del sujeto. En caso de existir dos entidades emisoras o dos sujetos con el mismo nombre, se puede utilizar este campo para desambiguar. Sin embargo, se ha probado que este mecanismo no es una solución satisfactoria. Actualmente el RFC 3280[20] no recomienda el uso de estos campos.
- **Extensions:** Este es un campo opcional y aparece únicamente en los certificados X.509 v3. Si el campo está presente, el certificado contiene una o m´as extensiones de certificado; cada extensión incluye un identificador de extensión, una bandera que indica si la extensi´on es crítica o no, y el valor de la extensi´on. Comúnmente, las extensiones de los certificados han sido definidas por ISO y ANSI y la razón de su existencia es proporcionar mayor flexibilidad al certificado digital. Cualquier organización puede definir una extensión privada para cumplir con sus requerimientos espec´ıficos. Esta flexibilidad crea un problema: un certificado digital creado bajo el estándar X.509 v3 puede no ser totalmente legible por las implementaciones que soportan certificados X.509 v3. Cuando una extensión de certificado no es conocida por la aplicaci´on que lo recibe, aparece la incompatibilidad. Esta es la razón de la existencia de la bandera indicando si una extensi´on es crítica o no lo es. Si es la extensi´on es marcada como no-crítica la aplicación lo único que hace es ignorar la extensión; por otra parte, si la extensi´on es marcada como crítica el resultado es que el certificado no puede ser utilizado debido a que se desconoce la funcionalidad de la extensión.

Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

1. Tipo de extensión. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
2. Valor de la extensión. Este subcampo contiene el valor actual del campo.

3. Indicador de importancia. Es un *flag* que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

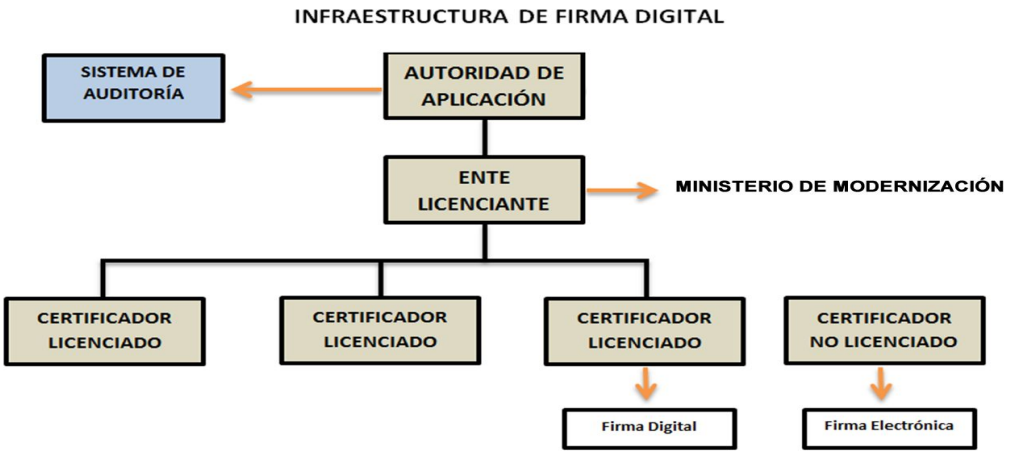
El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3:

- Limitaciones básicas. Este campo indica si el sujeto del certificado es una CA y el máximo nivel de profundidad de un camino de certificación a través de esa CA.
- Política de certificación. Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.
- Uso de la clave. Este campo restringe el propósito de la clave pública certificada, indicando, por ejemplo, que la clave sólo se debe usar para firmar, para la encriptación de claves, para la encriptación de datos, etc. Este campo suele marcarse como importante, ya que la clave sólo está certificada para un propósito y usarla para otro no estaría validado en el certificado.

El formato de certificados X.509 se especifica en un sistema de notación denominado *sintaxis abstracta uno* (*Abstract Syntax One* o ASN-1). Para la transmisión de los datos se aplica el DER (*Distinguished Encoding Rules* o *reglas de codificación distinguible*), que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales.

2.2.5. Infraestructura de firma digital en la República Argentina

La infraestructura de firma digital está compuesta por diversos actores que permiten la emisión de certificados para verificar las firmas en condiciones seguras desde el punto de vista técnico y legal.



2.4. Infraestructura de firma digital

Los entes certificadores que han obtenido su licencia de parte del Ministerio de Modernización son:

- ✓ Administración Federal de Ingresos Públicos (AFIP)
- ✓ Administración Nacional de la Seguridad Social (ANSES)
- ✓ Oficina Nacional de Tecnologías de Información (ONTI)
- ✓ Autoridades Certificantes para Personas Físicas y Jurídicas: ENCODE S.A.

Los siguientes se encuentran al 14/08/2017 en proceso de licenciamiento

- ✓ Corte Suprema de la Provincia de Buenos Aires
- ✓ Edicom SA
- ✓ Tecnología de Valores SA

2.2.6. Lista de revocación de certificados

Concepto

La lista de revocación de certificados, conocida como CRL , usualmente utilizada en una infraestructura de clave pública es una lista de certificados que han sido revocados, que ya no son válidos y, por ende, en lo que no debe confiar ningún usuario.

Para qué sirve

Cuando una autoridad certificante (CA) emite un certificado digital, lo hace con un período máximo de validez que oscila entre dos y cuatro años máximo. El objetivo de este período de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital.
Sin embargo, existen otras situaciones que pueden invalidar el certificado digital, aún cuando no ha caducado, y se mencionan a continuación:

- El usuario del certificado denuncia que su clave privada ha sido robada.
- Desaparece la condición por la que el certificado fue expedido.
- El certificado contiene información errónea o información que ha cambiado.
- Una orden judicial

Por lo que la CRL es un mecanismo que permite comprobar la validez de un certificado.

Como funciona

Una CRL[21] es una lista de números de serie de certificados digitales revocados por una CA concreta. Dicha lista está firmada digitalmente por la propia CA. Cuando un tercero desea comprobar la validez de un certificado debe descargar la CRL actualizada desde los servidores de la misma CA que emitió el certificado en cuestión. A continuación comprueba la autenticidad de la lista gracias a que la misma se encuentra firmada digitalmente. Después debe comprobar que el número de serie del certificado cuestionado esté en la lista. En caso afirmativo, no se deberá aceptar el certificado como válido.

Ventajas e inconvenientes

La ventaja más importante de las CRL es que se pueden consultar sin necesidad de una conexión de datos permanente con cada autoridad certificante.
Sin embargo las desventajas del uso de CRL son varias:

- Existe la posibilidad de que un certificado haya sido revocado, pero no aparezca en la CRL del tercero que comprueba su validez. Esto se debe a que la CRL puede no estar actualizada.
- Si existe responsabilidad legal por el uso de un certificado revocado, no hay forma de demostrar quién es el culpable: el tercero por no comprobar la validez o la autoridad certificante por no incluirlo en la CRL a tiempo.
- Las CRL solamente crecen en tamaño, lo que resulta ineficiente al momento de consultar por un sólo certificado.

2.2.7. Protocolo de comprobación del Estado de un Certificado en línea (OCSP)

OCSP[22] es un método para determinar el estado de vigencia de un certificado digital X.509 sin utilizar listas de revocación de certificados (CRL). Dicho protocolo se describe en el RFC 6960[23].
Los mensajes de OCSP se codifican en ASN.1[24] y habitualmente se transmiten sobre el protocolo HTTP.

Ventajas sobre las CRL:

- OCSP puede proporcionar información más adecuada y reciente del estado de revocación de un certificado.
- OCSP elimina la necesidad de que los clientes tengan que obtener y procesar la CRL, ahorrando tiempos de conexión y procesamiento.
- El contenido de las CRL puede considerarse información sensible y la misma es provista públicamente.
- Una consulta sobre el estado de un certificado sobre una CRL, debe recorrerla completa secuencialmente para decir si es válido o no. Un "OCSP responder" (Servidor OCSP) en el fondo, usa un motor de base de datos para consultar el estado del certificado solicitado, con todas las ventajas y estructura para facilitar las consultas. Esto se manifiesta aún más cuando el tamaño de la CRL es muy grande.

OCSP vs CRL

Una diferencia importante entre CRL y OCSP, es que una CRL puede ser almacenada temporalmente para hacer consultas locales, en cambio para usar OCSP se requiere de conexión con el "OCSP responder". Si bien la CRL está disponible sin conexión, mientras más tiempo esté sin actualizarse, se hace menos confiable la información que nos brinde, porque pueden haberse revocado algunos certificados entre actualizaciones.

Si se considera que se usa una CRL almacenada por un tiempo para ser consultada, versus el ancho de banda que se usa por cada consulta a través de OCSP, existe una diferencia de uso de ancho de banda que crece mientras aumenta el número de validaciones por día que debe responder la Autoridad Certificadora. Con CRL, el ancho de banda usado sigue una curva logarítmica, por el hecho de que aunque aumenten las consultas diarias, estas se hacen a la CRL almacenada. En cambio, con OCSP, si las consultas aumentan necesariamente aumenta el ancho de banda usado, por lo que la curva resultante es exponencial. Debido a esto, el tiempo de validación, a pesar de seguir la misma curva, al aumentar las validaciones por día, usando CRL, el tiempo "límite" es menor al que se obtiene si se usa OCSP.

2.2.8. Public-Key Cryptography standards (PKCS)

Es un conjunto de especificaciones técnicas desarrolladas por Netscape, RSA y otros, cuyo objetivo es definir criterios comunes para los protocolos de la criptografía pública[25]

Resumen de los estándares PKCS			
	Versión	**Nombre**	**Detalle**
PKCS#1	2.1	Estándar criptográfico RSA	Define estándares para la implementación del cifrado RSA. También define la sintaxis ASN.1 para la representación de claves e identificación de esquemas.
PKCS#2	-	*Obsoleto*	Definía el cifrado RSA de resúmenes de mensajes, pero fue absorbido por el PKCS#1.
PKCS#3	1.4	Estándar de intercambio de claves Diffie-Hellman	Describe un método para implementar el acuerdo clave de Diffie-Hellman, mediante el cual dos partes Pueden acordar una clave secreta que sólo es conocida por ellos
PKCS#4	-	*Obsoleto*	Definía la sintaxis de la clave RSA, pero fue absorbido por el PKCS#1.
PKCS#5	2.0	Estándar de cifrado basado en contraseñas	Proporciona un mecanismo para lograr una mayor seguridad en las primitivas criptográficas basadas en contraseñas, que cubren funciones en esquemas de cifrado, autenticación de mensajes, esquemas y sintaxis ASN.1. Este estándar se define en la RFC 2898 [26]
PKCS#6	1.5	Estándar de sintaxis de certificados extendidos	Define extensiones a la antigua especificación de certificados X.509 versión 1. La versión 3 del mismo lo dejó obsoleto.
PKCS#7	1.5	Estándar sobre la sintaxis del mensaje criptográfico	Define la sintaxis para firmar y/o cifrar mensajes en PKI. Fue la base para el estándar S/MIME, ahora basado en la RFC 3852 [27], una actualización del estándar CMS utilizado para firmar

			digitalmente, obtener el digest, autenticar, o cifrar arbitrariamente el contenido de un mensaje.
PKCS#8	1.2	Estándar sobre la sintaxis de la información de clave privada	Describe la sintaxis para la información de clave privada que incluye una clave para algún algoritmo de clave pública y un conjunto de atributos
PKCS#9	2.0	Tipos de atributos seleccionados	Define dos clases de objetos auxiliares donde se empaquetan nuevos atributos. También define nuevas reglas que pueden ser utilizadas en otros estándares.
PKCS#10	1.7	Estándar de solicitud de certificación	Define el formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública [28]
PKCS#11	2.20	Interfaz de dispositivo criptográfico	Define un API genérico de acceso a dispositivos criptográficos [29]
PKCS#12	1.0	Estándar de sintaxis de intercambio de información personal	Define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica[30].
PKCS#15	1.1	Estándar de formato de información de dispositivo criptográfico	Define un estándar que permite a los usuarios de dispositivo criptográficos identificarse con aplicaciones independientemente de la implementación del PKCS#11 cryptoki u otro API. RSA ha abandonado las partes relacionadas con la tarjeta IC de este estándar, subsumidas por el estándar ISO/IEC 7816-1

2.2.9 Timestamping

Es un servicio que permite demostrar que un conjunto de datos no han sido modificados desde un instante determinado de tiempo.
Dicho servicio [31] se basa en los mecanismos de firma digital y suele ser un servicio adicional que prestan las CA. En términos generales, se establece una tercera parte de confianza, objetiva, que es aceptada tanto por el emisor como por el receptor, y es la encargada de dar fe de la fecha y hora de una transacción. Es decir, agrega un nuevo dato, “tiempo”, a la transacción o al documento, por el cual las partes aceptan la validez temporal que se asocia a ese dato determinado.
Los estándares involucrados en el servicio de Timestamping son:

- RFC 3161 [32]: Especifica el formato de una solicitud enviada una TSA (Autoridad de certificación de Timestamping), así como también el formato de respuesta.
- RFC 3628 [33]: Define los requisitos que debe tener una política de sellado de tiempo para las TSA.
- ISO/IEC 18014: Específica diferentes técnicas de sellado en el tiempo.
- ANSI X9.95: Define los requisitos mínimos en cuestiones de seguridad del uso de los sellos de tiempo.

Capítulo 3

3. Notificaciones

3.1. Concepto

El concepto de notificación proviene de la voz “notificare”, derivada de notus "conocido" y de facere "hacer", en síntesis, quiere decir “hacer conocido”.
Como actividad procesal, la notificación[34] es la acción y efecto de dar a conocer al destinatario de la resolución, el contenido de la misma.
Los sujetos que participan en una notificación son dos: el organismo que hará la notificación y el destinatario de la notificación que quedará legalmente enterado de la comunicación cuando se cumplan los requisitos legales pertinentes.

3.2. Notificación. Acción y efecto de notificar

De acuerdo a la definición anteriormente mencionada, se puede realizar la siguiente distinción: notificar[34] siempre es un efecto, pero no siempre una acción. Es decir, que notificar no implica que el juez o las partes hagan algo con un fin específico, a veces simplemente se lo utiliza con fines informativos.
Existen casos en dónde la notificación se produce por mandato legal y la persona se da por notificada cuando llega el día de nota (martes o viernes[35]) más allá de lo que piense, diga o haga.
También puede ocurrir que la persona se dé por notificada realizando otro acto procesal, por ejemplo, al retirar un expediente en préstamo, se produce automáticamente la notificación de todas la resoluciones producidas hasta el momento.
Por último, existen las notificaciones por nota o realizadas personalmente, dónde se busca explícitamente que el destinatario de la resolución se dé por notificado.
En todos los casos mencionados puede ocurrir que exista una discrepancia entre la notificación en sí misma y la postura del notificado de acuerdo a cómo se deben contar los plazos procesales.

3.3. Clasificación de los modos de notificación

3.3.1. Teorías del “conocimiento” y de la “recepción”

Existen diversos criterios de clasificación de las modalidades de notificación, sin embargo podemos hacer una distinción de dos grandes “teorías”[36]: la del “conocimiento” y la de la “recepción”.

En la teoría del “conocimiento” para que la notificación sea considerada como tal es necesario que el destinatario de la resolución judicial la llegue a conocer efectivamente; en la teoría de la “recepción”, en cambio, lo importante no es el conocimiento (que puede llegar o no), sino el cumplimiento de ciertos aspectos legales al momento de producirse la actividad notificativa.
Como ya se definió, si notificación[34] significa “acción y efecto de hacer conocido”, el conocimiento no puede ser ajeno a ninguna teoría que explique el fenómeno. Si notificar es hacer conocido algo, el conocimiento debe ser un concepto que debe estar presente en cualquier teoría que explique lo que es una notificación.
Analizando ambas teorías[35], es importante destacar el dualismo entre la teoría de la recepción y la teoría del conocimiento, debido a que la teoría de la recepción también supone conocimiento desde que asume que el cumplimiento de las normas que regulan la notificación podrán producir probablemente el conocimiento de la resolución judicial.
En conclusión, si notificar es poner en conocimiento[34], no existe teoría que explique cómo se produce una notificación sin mencionar el concepto de conocimiento. Así, ambas teorías, son teorías del conocimiento.

3.3.2. Notificación Actual

La notificación actual es la que proporciona de forma directa al destinatario el conocimiento [34] de la resolución judicial.
En las notificaciones basadas en el conocimiento actual, el destinatario de la resolución es quien se presenta en persona con el objetivo de darse como notificado.
Dicha actividad notificativa reúne dos requisitos:

- El destinatario de la resolución es quien participa activamente para recibir la notificación.

- Pone en conocimiento de la resolución al destinatario.

3.3.3. Notificación bilateral

En esta modalidad de notificación[34] alguien pone la resolución en conocimiento de su destinatario. Esto ocurre en las llamadas notificaciones personales consentidas o notificaciones por cédula.

3.3.4. Notificación unilateral

En este caso, es el destinatario de la resolución quien, de alguna manera declara conocimiento de la misma.
Una notificación unilateral[34] puede ser:

- **Expresa:** si el destinatario asume un rol activo y pone en manifiesto el conocimiento que tiene acerca de la resolución.
- **Implícita:** si el destinatario despliega cualquier actividad procesal que haga presuponer el conocimiento de la misma.

3.4. Gobierno Electrónico

Es la aplicación de tecnologías de información al funcionamiento del sector público, con el objetivo de incrementar la eficiencia, transparencia y participación ciudadana[37].
Esta definición expresa claramente cómo a través de su enfoque innovador, las acciones del gobierno electrónico sitúan las TICs como elementos de apoyo y pone énfasis en el desarrollo de un buen gobierno. Esto implica alcanzar mayores niveles de eficiencia y eficacia en el trabajo gubernamental, mejorando los procesos y procedimientos del gobierno, aumentando la calidad de los servicios públicos, incorporando más y mejor información en los procesos decisorios y facilitando la coordinación entre las diferentes instancias de gobierno.

3.4.1. Fases del Gobierno electrónico

El desarrollo del gobierno electrónico (GE) [37] es un proceso evolutivo, que en cada una de sus etapas persigue diferentes objetivos y tiene requerimientos disímiles en cuanto capacitación en el uso de tecnologías, necesidades cognitivas y costos que deben asumirse.
Suelen diferenciarse cuatro fases:

- **Presencia**: implica poner en línea de información a los que pueden acceder los ciudadanos y las empresas, pero sin interacción.
  Consiste en la creación de un portal institucional, lo que implica utilizar Internet para hacer disponible información de interés que fluye en un sólo sentido. Esta instancia no posibilita la interacción con la ciudadanía.

- **Interacción**: se abren canales de comunicación tales como contactos de correo, envíos de formulario. Permite una comunicación en ambos sentidos. El ciudadano tiene la posibilidad de proporcionar una dirección de email, desde la cual puede realizar consultas, obtener información y efectuar reclamos, generando así las primeras interacciones con el gobierno e incrementando la participación ciudadana.

- **Transacción:** en esta fase, se encuentran las instituciones más avanzadas en materia de tecnología, se han incorporado aplicaciones de autoservicio para que el ciudadano pueda realizar trámites completos en línea.

- **Transformación:** consiste en una integración total entre agencia, el sector privado y la ciudadanía, ofreciendo servicios cada vez más personalizados. En esta etapa surgen conceptos como el de *ventanilla única*.

3.4.2. Beneficios del Gobierno Electrónico

➢ **Beneficios para los ciudadanos**

Con respecto a los ciudadanos, el gobierno tiene como desafío innovar e invertir en nuevos modelos de gobierno, de manera que los servicios entregados proporcionen formas más eficientes, convenientes, fáciles y económicas para el ciudadano. La personalización de los servicios debe hacer posible la inclusión de todo tipo de personas.
El sector público y el privado deben colaborar, aumentando la capacidad para usar la información y así conseguir mayores ventajas para el ciudadano. En el mundo de los negocios es vital establecer y mantener la confiabilidad de la información. Todo esto debe ir acompañado de normas que aseguren la privacidad, seguridad y confidencialidad de la información de los individuos. Asimismo el GE permite que las personas tengan mayor acceso a la información, haciendo más participativa la democracia del país y permitiendo la retroalimentación del gobierno con las propuestas hechas por los ciudadanos.
La vida de la mayoría de las personas se ha visto revolucionada debido a los desarrollos de tecnología, la reducción en los costos de las comunicaciones, el surgimiento de nuevos servicios y las nuevas formas de llevar a cabo los existentes. Esto ha permitido una mejora en el nivel de vida de los ciudadanos, ya que permite:

- Mejor acceso, con servicios que son entregados donde y cuando se necesitan.

- Mayor variedad de medios para la distribución del servicio.

- Segmentación del mercado, con servicios enfocados a las necesidades del ciudadano individual.

- Una respuesta sobre la satisfacción del ciudadano frente al servicio entregado.

La transformación del gobierno debe ser una oportunidad para la inclusión social, desapareciendo las limitantes geográficas aumentando la comunicación y oportunidades de trabajo. Para poder lograr eso, deben crearse facilidades para que los ciudadanos puedan familiarizarse con los cambios tecnológicos.

➢ **Beneficios para las empresas:**

Una de las razones por la cual los negocios electrónicos han tomado gran importancia, es porque las técnicas del comercio electrónico administran las relación de proveedores y clientes. El sector público se debe alinear de igual forma para poder recibir los beneficios de menores costos y mejores posibilidades de abastecimiento, lo que beneficia tanto al sector público como a los empresarios.
El sector público no sólo interactúa con los comerciantes jugando el papel de proveedor o cliente. Es además el responsable de una gran variedad de normas y funciones de apoyo. El sector empresarial requiere que se le brinde apoyo en los inicios de sus negocios, en la expansión de los mismos o simplemente en llevar el negocio adelante de una forma más fácil y accesible. Toda esta facilitación es posible con la implantación del GE y la introducción de la cultura necesaria que lleva implícita esta nueva forma de gobernar.
Los beneficios para las empresas en el GE deben asegurarse teniendo en consideración ciertos factores tales como:

- **Seguridad:** las transacciones realizadas por medios electrónicos deben ofrecer la seguridad necesaria para que las empresas puedan participar.

- **Eficiencia y costos:** los sistemas deben cumplir los requerimientos para que las empresas puedan operar a igual o menor costo, e igual o mayor eficiencia que la forma tradicional.

➢ **Beneficios para el gobierno:**

El GE propone una reestructuración y un rediseño en los métodos de trabajo del gobierno, ofreciendo beneficios para los negocios internos del Estado. Esto incluye ganancias en eficiencia y efectividad por la mejor utilización de la información y el mejor manejo de programas de trabajo. Por ejemplo, una intranet puede ofrecer la posibilidad de brindar un conocimiento común y que cruce de manera transversal a la organización.

3.5. Gobierno abierto

El gobierno abierto es un concepto más amplio que el de gobierno electrónico, que permite a los ciudadanos colaborar y participar activamente en la creación y mejora de los servicios públicos, haciendo énfasis en la transparencia.

Los ejes fundamentales del gobierno abierto son:

- Transparencia
- Colaboración
- Participación

La publicación de los datos públicos que otras áreas de gobierno y ciudadanos puedan utilizarlos impulsando la innovación, desarrollo económico, generación de conocimiento científico y mejora en los servicios públicos

3.6. Notificación electrónica

Las notificaciones electrónicas son aquellas comunicaciones que emite la administración pública y privada utilizando medios electrónicos. En el campo de la Administración de Justicia, surgen como una alternativa inmediata para lograr que los procesos judiciales que utilicen este medio se desarrollen con una mayor celeridad, economía y seguridad procesal.
A través de las notificaciones electrónicas aplicadas, los responsables podrán enterarse del contenido de las resolución, entre otras, desde la comodidad de su hogar, oficina, sin necesidad de desplazarse a las sedes o domicilios procesales y sin la obligación de adquirir cédulas de notificación; Es decir ahorrando tiempo y dinero.

3.7. Domicilio electronico

El domicilio electrónico (DE) se define como un espacio virtual, en donde la persona recibe sus notificaciones electrónicas. Dicho espacio tiene, en el ámbito administrativo público, los mismos efectos del domicilio fiscal constituido, siendo válidas y plenamente eficaces todas las notificaciones, emplazamientos y comunicaciones que allí se produzcan.
Anteriormente cada vez que cualquier entidad del estado debía comunicar o solicitar información a un ciudadano, era indispensable que la persona se acercara al organismo público personalmente, implicando traslados, dinero e impacto ambiental.
Mediante el DE se da un paso cualitativo en la modernización de la gestión pública, permitiendo que toda la comunicación con el ciudadano se haga a través de mecanismos electrónicos.
Los beneficios concretos del uso del DE son:

- ***Ahorro de tiempo:*** *p*ermite al ciudadano recibir comunicaciones y notificaciones electrónicas sin necesidad de desplazarse personalmente al organismo notificador.

- ***Ahorro de costos:*** *n*o requiere gastos de traslado de personas ni de papeles, ni de almacenamiento, ni de personal para atender a los notificados.

- ***Impacto ambiental:*** *e*limina desplazamientos de personas y de documentos en papel. Elimina la necesidad de imprimir papel (ahorro en impresoras, insumos, energía).

3.8. Notificación Electrónica. Antecedentes

3.8.1. Corte Suprema de Justicia de la Nación

En el año 2007 la Corte Suprema de Justicia de la Nación[38] creó la Comisión Nacional de Gestión Judicial encabezada por su presidente, Ricardo Lorenzetti e integrada por jueces de todo el país.
Esta comisión se encargó de delinear políticas estratégicas y planes operativos para impulsar el rediseño de la organización del Poder Judicial mediante la incorporación de nuevas tecnologías y criterios de gestión.

En su labor plantearon el paradigma de reconocer a la gestión judicial como herramienta de apoyo a la labor de los jueces, así como la búsqueda de una mejora contínua en el trabajo que diariamente cumplen magistrados, funcionarios, empleados, abogados y auxiliares.
Definieron que los objetivos de la gestión judicial se centrarán en los siguientes ejes:

- Gestión administrativa organizacional - Rediseño de procesos.

- Coeficiente de gestión judicial.

- Firma digital.

- Notificación electrónica.

- Expediente digital.

Entre los proyectos que implementaron se encuentran: un plan de acceso electrónico a la información, sistema informático de gestión de la Corte Suprema de Justicia, aplicación de instructivos de gestión, expediente digital y notificación electrónica.

Sistema de notificaciones

En julio de 2011 se sancionó y promulgó la Ley Nacional Nº 26.685[39] que contiene sólo 3 artículos, en el primero, autoriza la utilización de expedientes electrónicos, documentos electrónicos, firmas electrónicas, firmas digitales, comunicaciones electrónicas y domicilios electrónicos constituidos, en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales.

En el artículo segundo establece que la Corte Suprema de Justicia de la Nación y el Consejo de la Magistratura de la Nación, de manera conjunta, reglamentarán su utilización y dispondrán su gradual implementación.
De acuerdo a este mandato y por medio de la Acordada 31/2011[40] la Corte Suprema reglamentó el sistema de notificaciones electrónicas.

La Acordada establece que a partir de su entrada en vigencia, toda persona que litigue por propio derecho o en ejercicio de una representación legal o convencional deberá constituir domicilio electrónico para las causas judiciales que tramiten ante la Corte Suprema de Justicia de la Nación.
Por medio de la acordada 38/2013[41] la Corte Suprema de Justicia de la Nación extendió a todo el Poder Judicial la aplicación del sistema de notificaciones electrónicas.

Según esta disposición, desde el 18 de noviembre de 2013 el sistema de notificación electrónica se aplicará a todas las causas en que se tramiten los escritos de interposición de recursos ante las cámaras nacionales y federales y en las causas que pasen a instancia de juicio en los tribunales orales en los que el programa de gestión judicial se encuentre implementado.
Establece también que a partir del 1° de abril de 2014, la notificación electrónica será instaurada de manera obligatoria para todas las causas que se promuevan en todos los juzgados y tribunales de las cámaras nacionales y federales.
El sistema de notificaciones electrónicas del Poder Judicial de la Nación reemplaza las notificaciones de providencias, resoluciones y sentencias que deban practicarse personalmente o por cédula al domicilio constituído.
Permite confeccionar cédulas vía internet, y realizar su gestión enviando la notificación al Juzgado y a los letrados de las partes, admite adjuntar archivos con la extensión PDF, TIFF y JPG.
Los destinatarios de la Notificación Electrónica pueden ser los letrados apoderados, patrocinantes y/o defensores, así como los Fiscales, Defensores Oficiales, Peritos y todo aquel que actúe en un proceso judicial en calidad de interviniente.

Funcionamiento

Los letrados intervinientes en un proceso judicial deben constituir domicilio electrónico(DE), el cual se define como un espacio virtual seguro, personalizado y válido, registrado por personas para la entrega o recepción de comunicaciones de cualquier naturaleza.
Su constitución, se lleva a cabo completando un formulario en el sitio web de la Corte Suprema de Justicia de la Nación, en el que además deben cargar distintos archivos, una foto en formato jpg, matrícula profesional, DNI y constancia de inscripción CUIT o CUIL en formato pdf.
Luego de completar el formulario con todos sus requisitos, deben acreditar su identidad los Tribunales Federales o en la mesa de entradas de la Corte Suprema de Justicia de la Nación.

3.8.2 Corte Suprema de Justicia de la Provincia de Buenos Aires

Como primer avance sobre la decisión de revisar el sistema de notificaciones, encontramos que en el año 2000, por Resolución 1991/00, la Suprema Corte de Justicia de la provincia creó una Comisión para la Optimización de las Notificaciones Judiciales, integrada por los reconocidos juristas y representantes de la Asociación Judicial Bonaerense.
La mencionada comisión elaboró informes que coincidían en la necesidad de contar con un sistema de notificaciones por vía digital. En aquel momento las propuestas consideraban reemplazar la cédula en papel por un correo electrónico y cambiar el domicilio tradicional por uno electrónico.
En el año 2007, se tramitó ante la Suprema Corte una iniciativa de modificación de la repartición encargada de dirigir los subsistemas de receptoría general de expedientes, archivos, mandamientos y notificaciones.
Para el estudio de esta iniciativa el máximo Tribunal dispuso la creación de una Comisión destinada al análisis y evaluación de la propuesta, en atención a la complejidad y variedad de cuestiones involucradas en la misma (Resolución 800/07 del 11 de abril de 2007), ampliándose su integración por Res. 1457/07 del 20 de junio de 2007, oportunidad en que se le encomendó además la elaboración de un plan de implementación de notificaciones electrónicas en la provincia de Buenos Aires.

En el informe elaborado por la comisión se examinaron diversas variantes de notificación, teniendo en cuenta la estructura vigente y los sistemas de gestión utilizados en los distintos tribunales.
Los sistemas considerados viables fueron dos, por un lado en el envío de correos electrónicos firmados digitalmente a domicilios constituidos por las partes en sus escritos iniciales; y por el otro la utilización de un sitio web para almacenar y gestionar en forma segura la información del proceso de notificación.

Este último fue el sistema elegido por la Suprema Corte, que mediante Acuerdo 3399, en noviembre de 2008 aprobó la reglamentación de una prueba piloto que comenzó a funcionar en tres Juzgados y autorizó que se pueda ampliar por resolución del Presidente.
Paulatinamente se fueron sumando a la prueba otros Juzgados Civiles y Comerciales, Juzgados de Familia, Tribunales de Trabajo, Juzgados en lo Contencioso Administrativo, Juzgados de Paz y Cámaras de Apelación y Garantías en lo Penal de toda la provincia.
El sistema implementado mediante la prueba piloto reemplazó la modalidad tradicional de diligenciar las cédulas dirigidas a domicilios constituidos, no así a las dirigidas al domicilio real o denunciado como es el caso del traslado de la demanda.

Sistema de notificaciones

Luego del éxito obtenido con la prueba piloto, y de la sanción de la Ley provincial N° 14.142 que modifica el Código Procesal Civil y Comercial de la provincia de Buenos Aires habilitando la utilización de medios electrónicos para la notificación, la Suprema Corte de Justicia de la Provincia de Buenos Aires aprobó mediante Acuerdo 3540/11, la “Reglamentación para la notificación por medios electrónicos”.
En la citada reglamentación se establece que la notificación de las resoluciones que, de conformidad con las disposiciones vigentes, deban ser diligenciadas a las partes o sus letrados y a los auxiliares de justicia en su domicilio constituido, podrá ser concretada a través de los mecanismos electrónicos previstos. En el año 2007, se tramitó ante la Suprema Corte una iniciativa de modificación de la repartición encargada de dirigir los subsistemas de receptoría general de expedientes, archivos, mandamientos y notificaciones.
Para el estudio de esta iniciativa el máximo Tribunal dispuso la creación de una comisión destinada al análisis y evaluación de la propuesta, en atención a la complejidad y variedad de cuestiones involucradas en la misma (Res. 800/07 del 11 de abril de 2007), ampliándose su integración por Res. 1457/07 del 20 de junio de 2007, oportunidad en que se le encomendó además la elaboración de un plan de implementación de notificaciones electrónicas en la provincia de Buenos Aires.

En el informe elaborado por la comisión se examinaron diversas variantes de notificación, teniendo en cuenta la estructura vigente y los sistemas de gestión utilizados en los distintos tribunales.
Los sistemas considerados viables fueron dos, por un lado en el envío de correos electrónicos firmados digitalmente a domicilios constituidos por las partes en sus escritos iniciales; Y por el otro la utilización de un sitio web para almacenar y gestionar en forma segura la información del proceso de notificación.
Este último fue el sistema elegido por la Suprema Corte, que mediante el acuerdo 3399, en noviembre de 2008 aprobó la reglamentación de una prueba

piloto que comenzó a funcionar en tres Juzgados y autorizó que se pueda ampliar por resolución del Presidente.
Paulatinamente se fueron sumando a la prueba otros Juzgados Civiles y Comerciales, Juzgados de Familia, Tribunales de Trabajo, Juzgados en lo Contencioso Administrativo, Juzgados de Paz y Cámaras de Apelación y Garantías en lo Penal de toda la provincia.
El sistema implementado mediante la prueba piloto reemplazó la modalidad tradicional de diligenciar las cédulas dirigidas a domicilios constituidos, no así a las dirigidas al domicilio real o denunciado como es el caso del traslado de la demanda.

Capítulo 4

4. Proyecto del HTC para notificación electrónica

4.1. Contexto

El *HTC* es un organismo de control externo de la hacienda pública, encargado de examinar las cuentas de percepción e inversión de las rentas públicas, tanto provinciales como municipales. Sus atribuciones están establecidas en la *Constitución de la Provincia de Buenos Aires que en el artículo 159 [42]* textualmente dice:
“La Legislatura dictará la Ley Orgánica del Tribunal de Cuentas. Éste se compondrá de un presidente abogado y cuatro vocales contadores públicos, todos inamovibles, nombrados por el Poder Ejecutivo con acuerdo del Senado. Podrán ser enjuiciados y removidos en la misma forma y en los mismos casos que los jueces de las Cámaras de Apelación. Dicho tribunal tendrá las siguientes atribuciones:

a. Examinar las cuentas de percepción e inversión de las rentas públicas, tanto provinciales como municipales, aprobarlas o desaprobarlas y en este último caso, indicar el funcionario o funcionarios responsables, como así también el monto y la causa de los alcances respectivos.

b. Inspeccionar las oficinas públicas provinciales o municipales que administren fondos públicos y tomar las medidas necesarias para prevenir cualquier irregularidad en la forma y con arreglo al procedimiento que determine la Ley. Las acciones para la ejecución de las resoluciones del Tribunal corresponderá al fiscal de Estado.

De manera supletoria, las acciones de fiscalización son regidas por la *Ley 10869 [43] Orgánica del Tribunal de Cuentas*, enunciando las siguientes facultades:

- Examinar los Libros de Contabilidad y la documentación existente en las dependencias públicas provinciales o comunales o en aquellos entes que de cualquier forma perciban, posean o administren fondos o bienes fiscales.

- Inspeccionar las mismas.

- Realizar arqueos de Caja.

- Efectuar la comprobación sumaria de los hechos delictuosos cometidos en la inversión de los fondos públicos.

- Celebrar convenios con Organismos similares de otras jurisdicciones para la fiscalización conjunta de Entes Interestaduales, sujetos a su competencia.

- Toda otra actividad que coadyuve al cumplimiento de las funciones previstas en la presente ley.

Para su funcionamiento cuenta con:

- Sede central, sita en la Torre Administrativa Gubernamental II, en la Ciudad de La Plata.

- 4 Delegaciones, sitas en La Plata, para estudio de Entes pertenecientes a la Vocalía de Administración Central.

- 4 Delegaciones, sitas en La Plata, para estudio de Entes Autárquicos.

- 20 Delegaciones para el estudio de las cuentas municipales, distribuidas en las siguientes localidades de la Provincia: 25 de mayo, Avellaneda, Azul, Bahía Blanca, Chascomús, Dolores, Junín, Ituzaingó, La Plata, Lomas de Zamora, Mar del Plata, Mercedes, Morón, Pehuajó, Pigé, Quilmes, San Isidro, San Justo, Vicente López y Zárate].

4.1.1 Certificación ISO

El Honorable Tribunal de Cuentas de la Provincia de Buenos Aires desde el año 2004 ha asumido un fuerte compromiso con la calidad de la gestión de sus procesos yha instalado la mejora continua como filosofía del trabajo.Para ello implementó un Sistema de Gestión de la Calidad conforme a la Norma ISO 9001 como marco y guía para la obtención de los objetivos de excelencia institucionales.
La primera certificación de la Norma fue obtenida el 16 de diciembre de 2004 con la ISO 9001:2000, y a partir de allí se ha mantenido anualmente certificando en el año 2009 con la ISO 9001:2008.

En el 2011, en busca de la eficiencia de la mejora continua, se gestionó y aprobó ante el Poder Ejecutivo Provincial una nueva Estructura Orgánico-funcional, incluyendo un sector denominado Dirección General de Gestión de la Calidad dentro de la Secretaría de Modernización y Fortalecimiento Institucional. La misión de dicha dirección es mantener la mejora continua a partir del desarrollo de programas, proyectos y sistemas relacionados con la Organización. Tiene a su cargo la elaboración, diseño y supervisión de la realización de las auditorías internas de la calidad del Organismo.

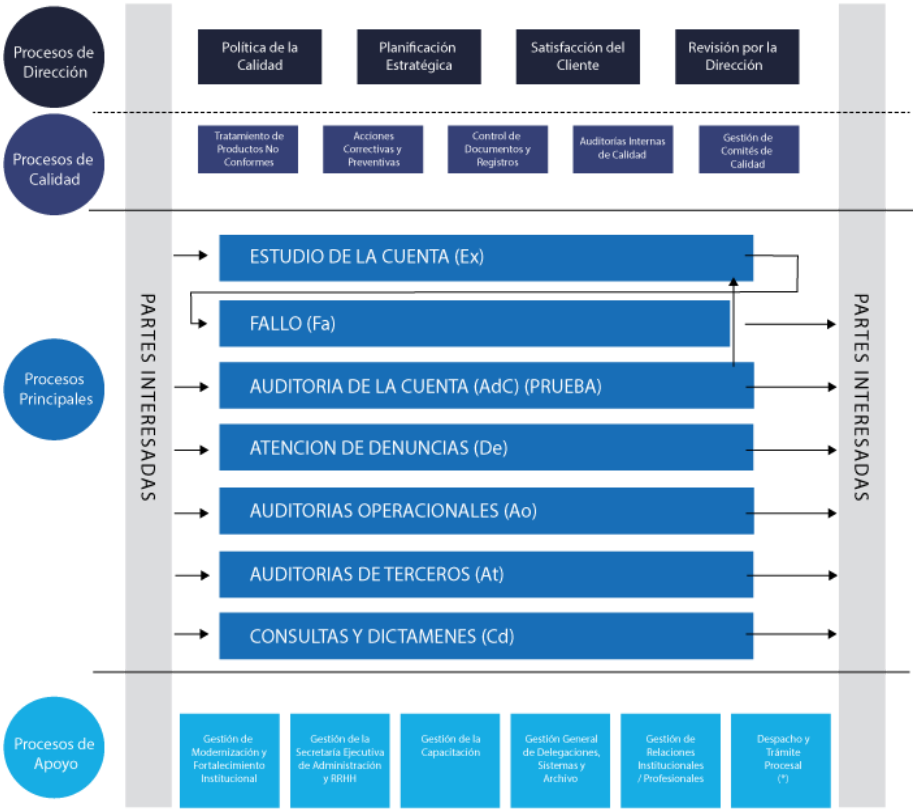
A través del decreto de creación de la Dirección de Calidad, se establecieron 5 Regiones Descentralizadas, cada una de ellas concentrando el asesoramiento de 4 Delegaciones Municipales.

Conjuntamente con las certificaciones, se implementaron soluciones automatizadas para la gestión de no conformidades, productos no conformes y archivos. La última solución desarrollada fue denominada “Yuran”[44] y se definió como la facilitadora de la comunicación y el conocimiento de todos los procesos y procedimientos documentados que exige el estándar ISO 9001.

A continuación se visualizan los procesos del HTC, clasificados en procesos de dirección, calidad, principales y de apoyo. Particularmente la Dirección de Sistemas tiene injerencia en el proceso “Gestión General de Delegaciones, Sistemas y archivos”.

DETERMINACIÓN DE PROCESOS

Honorable Tribunal de Cuentas
Provincia de Buenos Aires



(*) Se entiende que el proceso de Despacho y trámite procesal ayuda a la realización de todos los procesos del diagrama.

4.2. Inicio del proyecto de Notificación Electrónica

A principios del año 2015 comenzó a gestarse el proyecto de Notificación electrónica dentro del HTC, el cual debía abordarse como de alto impacto para el organismo. Dicho cambio posee injerencia sobre tres ejes fundamentales: actores o personas intervinientes, los procesos requeridos y herramientas tecnológicas que debían implementarse.
Las principales ventajas de la tecnología a destacar son:

- Reemplazar la documentación en papel por su equivalente en formato digital.
- Reducir los costos generales.
- Mayor celeridad y calidad en el proceso de notificación.
- Incrementar la velocidad de procesamiento.

- Reducir los tiempos operativos.

- Contribuir al desarrollo del Gobierno Electrónico.

Se justifica la aseveración de alto impacto reflexionando sobre el total de 8800 cuentadantes[1] distribuidos en más de 300 entes de estudio en el ámbito provincial como municipal.
Los actores internos que intervienen en dicho proceso son los usuarios de las 20 delegaciones de las vocalías de Municipalidades A y B, de las 8 delegaciones de las VocalÍa Central y Autárquicas y por último las relatorías que interactúan directamente con sus entes de estudio.

La definición formal del proyecto involucró la conformación de una Comisión, con carácter transversal a la organización e interdisciplinaria. Se combinaron actores de áreas vinculadas con Informática, Estudios de la Cuenta, Consultas y Modernización.
Las primeras actividades de la comisión consistieron en analizar los procesos de Notificación Electrónica de la Corte Suprema de la Provincia de Buenos Aires y ARBA y vincularlos con las necesidades propias del organismo teniendo en cuenta las particularidades de la actividad del Control.
Del análisis inicial surgieron tres componentes, considerados indispensables para la ejecución de este proceso. Los mismos, serán detallados a continuación.

4.3. Componentes

Declaración Jurada - DJW

Domicilio Electrónico

Mesa de Ayuda

4.3.1. Declaración Jurada Web (DJW)

[1] Funcionario o empleado público responsable de administrar fondos públicos dentro del ámbito de la Provincia de Buenos Aires, controlado por el HTC.

La Declaración Jurada Web es un formulario web que constituye el primer paso para lograr el ingreso del cuentadante al circuito del proyecto de notificación electrónica. El mismo se desglosa en 5 secciones:

- **Datos personales (**Fig. 5.1): contiene datos del cuentadante que no son pasibles de ser modificados, tales como su nombre, apellido, DNI, nacionalidad, entre otros. Además se compone de otros datos que pueden sufrir modificaciones, tal como el ente al que pertenece, el cargo y su dirección de correo electrónico.

- **Domicilio legal.** (Fig. 5.2)**:** aquel en el que el funcionario ejerce sus funciones.

- **Domicilio constituido.** (Fig.5.3): donde se cursarán las notificaciones por parte del HTC, conforme a los establecido en el Art. 8 de la resolución 7/2015[4].

- **Domicilio Real.** (Fig. 5.4): aquel donde reside en forma permanente.

- **Casillas de verificación** para optar adherirse como voluntario al sistema de notificaciones electrónicas a partir de 2017 y para extender dicha DJW a todos los ejercicios. (Fig. 5.5)

Fig. 5.1. Datos personales

Fig. 5.2. Domicilio Legal

Fig. 5.3. Domicilio Constituido

Fig.5.4. Domicilio Real

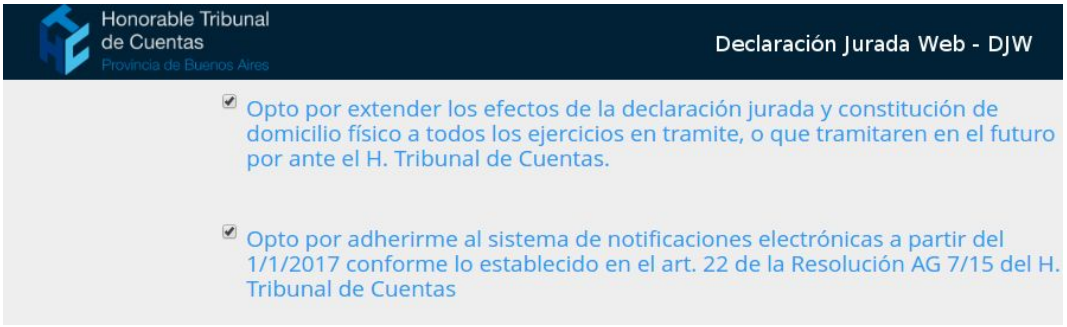


Fig.5.5. Opto

4.3.2. Domicilio electrónico

En base a la definición de domicilio electrónico realizada en la sección 3.7 del presente documento, vale aclarar que el HTC considera a Agosto de 2017 sólo dos tipos de notificaciones a recibir por el cuentadante:

- Aquellas en las que sí se explicita un plazo legal y poseen mayor rigor jurídico acorde a lo especificado en la sección 3.1, denominadas ***notificaciones.***

- Aquellas que no tienen definido un plazo legal, denominadas ***comunicaciones.***

Acceso

Para ingresar al domicilio electrónico el cuentadante debe dirigirse al sitio web del organismo, en la sección notificación electrónica (Fig. 5.6).

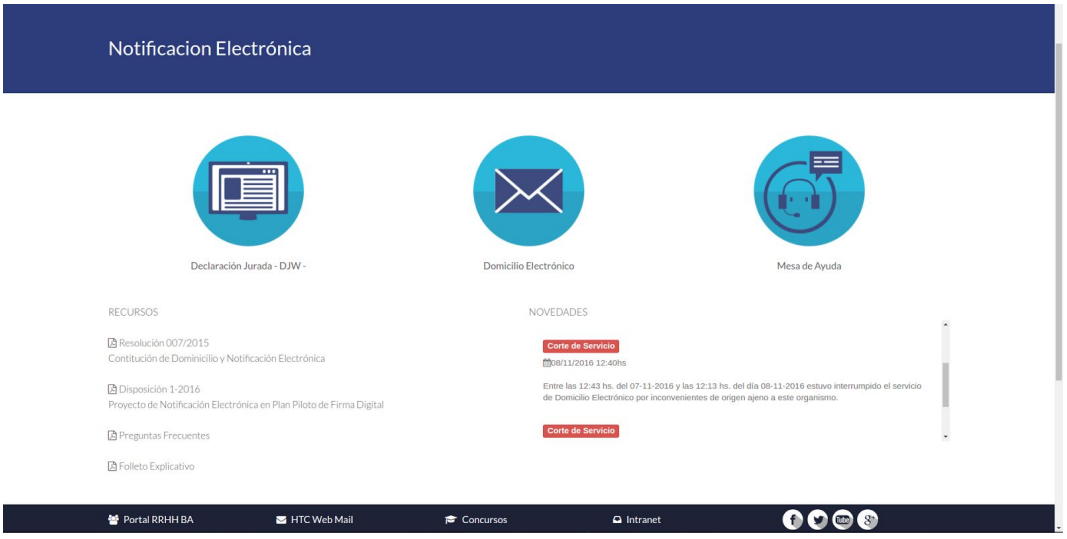


Fig.5.6. Sección de Notificación Electrónica en la web del HTC.

Dentro de dicha sección debe ingresar a “Domicilio Electrónico” y se visualizará la pantalla de login (Fig 5.7).

Fig. 5.7. Login en DE

Proceso de activación del Domicilio Electrónico

El proceso de activación requiere de una serie de pasos, los cuales se grafican en la fig. 5.8, a saber::

1. Cargar la DJW mediante el formulario mencionado anteriormente.
2. Imprimir dos copias de la DJW, adjuntar fotocopia del DNI y presentarlas ante la autoridad certificante de su ente.
5. Recibe el CADE (Comprobante de asignación de Domicilio Electrónico).
6. Ingresa a su mail declarado en la DJW, en el cual recibe su usuario y contraseña para acceder a su DE.
7. Accede a su DE por primera vez. Debe cambiar su clave obligatoriamente.

Por su parte, el HTC debe realizar una serie de pasos para que el cuentadante pueda activar su DE exitósamente:

3. Recibe la DJW y la fotocopia de DNI del cuentadante.
4. Valida la presentación de la DJW para verificar que los datos son correctos y genera el CADE correspondiente que es entregado al cuentadante. Por último envía el mail con el usuario y contraseña para que responsable active su DE.

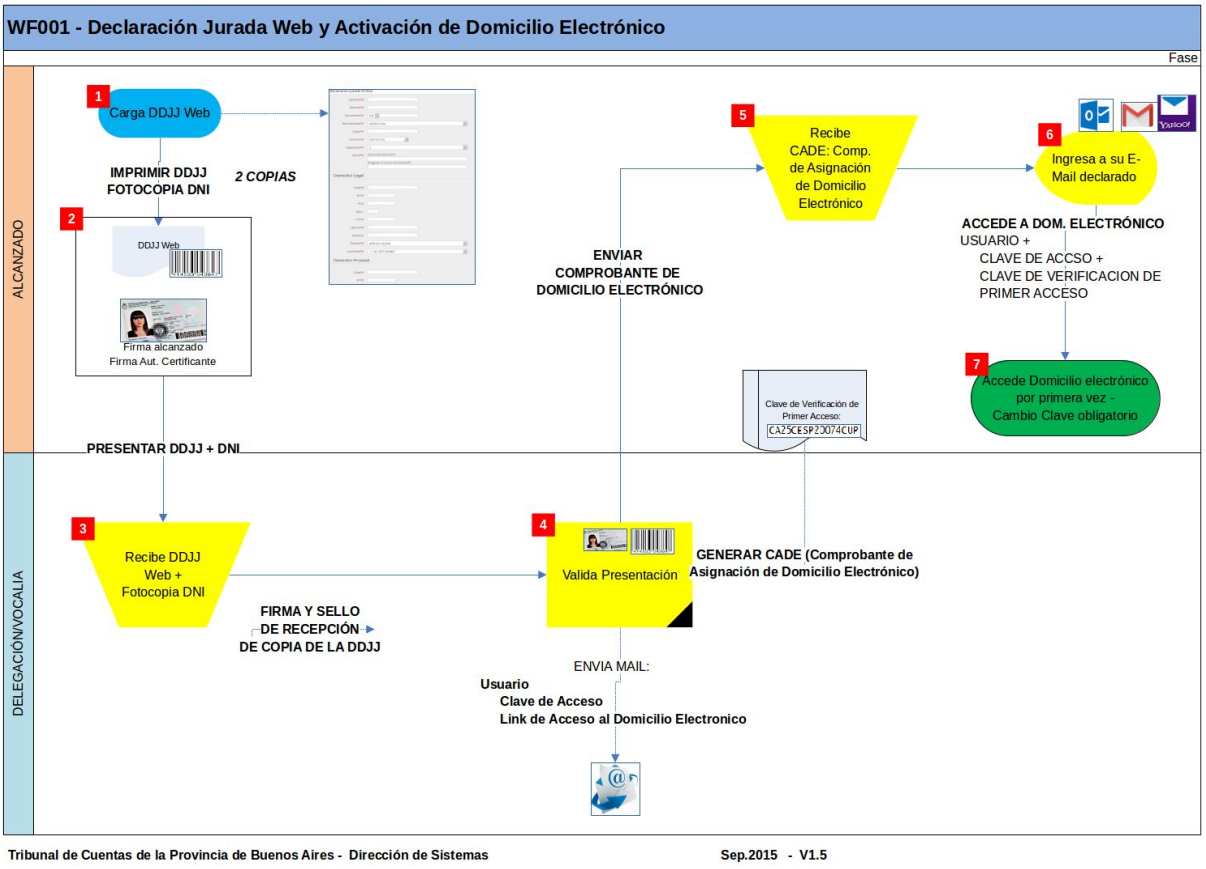


Fig. 5.8. Activación de Domicilio Electrónico

Descripción funcional del Domicilio Electrónico

Una vez que el cuentadante inicia sesión en su DE se le presenta la pantalla principal del mismo (Fig. 5.9). La misma está formada por 4 componentes:

- Novedades: Listado de novedades publicadas por el HTC que tienen relevancia para los usuarios del DE.

- Mis Declaraciones Juradas: Aquí se pueden visualizar el estado de últimas declaraciones juradas presentadas ante el HTC.

- Mis Datos: Resumen de los datos personales validados por el HTC.

- Mi Buzón: Resumen de las notificaciones y comunicaciones enviadas por el HTC.

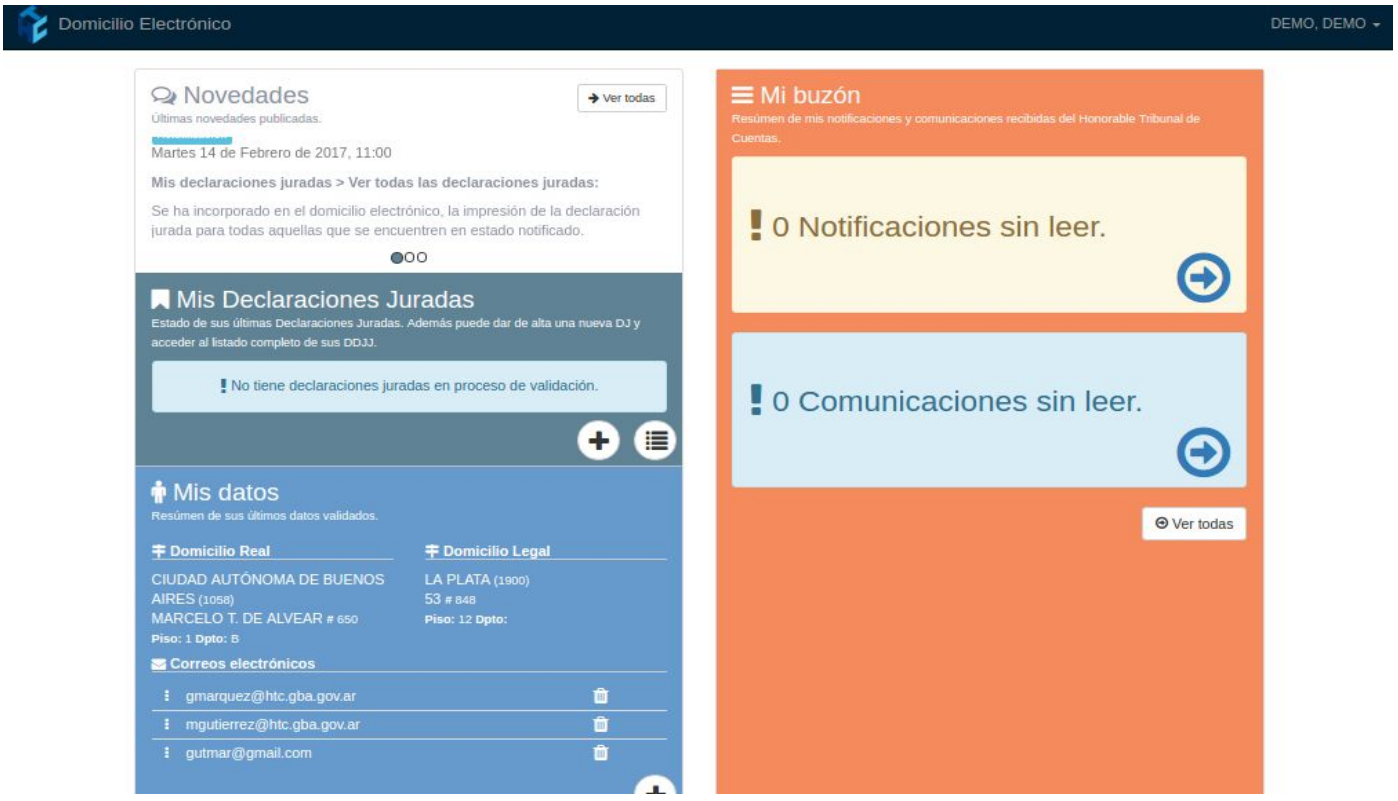


Fig. 5.9. Pantalla principal del DE

El componente principal del DE se denomina “Mis Declaraciones Juradas”. En este módulo el usuario puede ver sus declaraciones juradas cargadas en el sistema y agregar nuevas.
En la figura 5.10 se visualiza el listado de DDJJ web cargadas en el sistema, en donde pueden observarse distintos campos:

- Fecha de Presentación: de la DJW ante el HTC.
- Fecha de Notificación: Fecha en la que el cuentadante fue notificado por el HTC.
- Ente: Organismo en el que desempeña sus funciones.
- Cargo: Función que desempeña en el ente declarado.
- Domicilio Constituido
- Estado: Indica el estado en el que se encuentra la declaración jurada cargada. Éstos pueden ser:
    - En proceso.
    - Invalidada.
    - Anulada.

- Completada

- Ejercicio/s: Indica/n si el cuentadante ha optado por extender la DJW para todos los ejercicios o algunos.

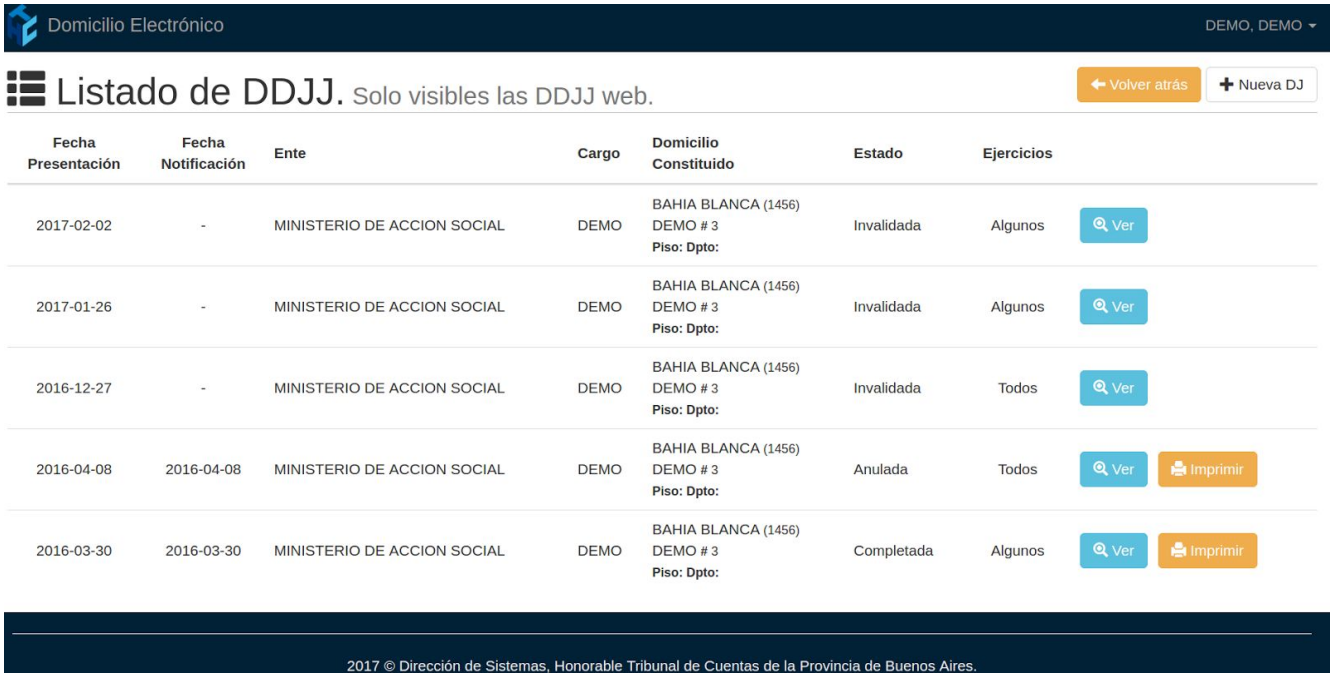


Fig. 5.10. Listado de DDJJ Web del cuentadante

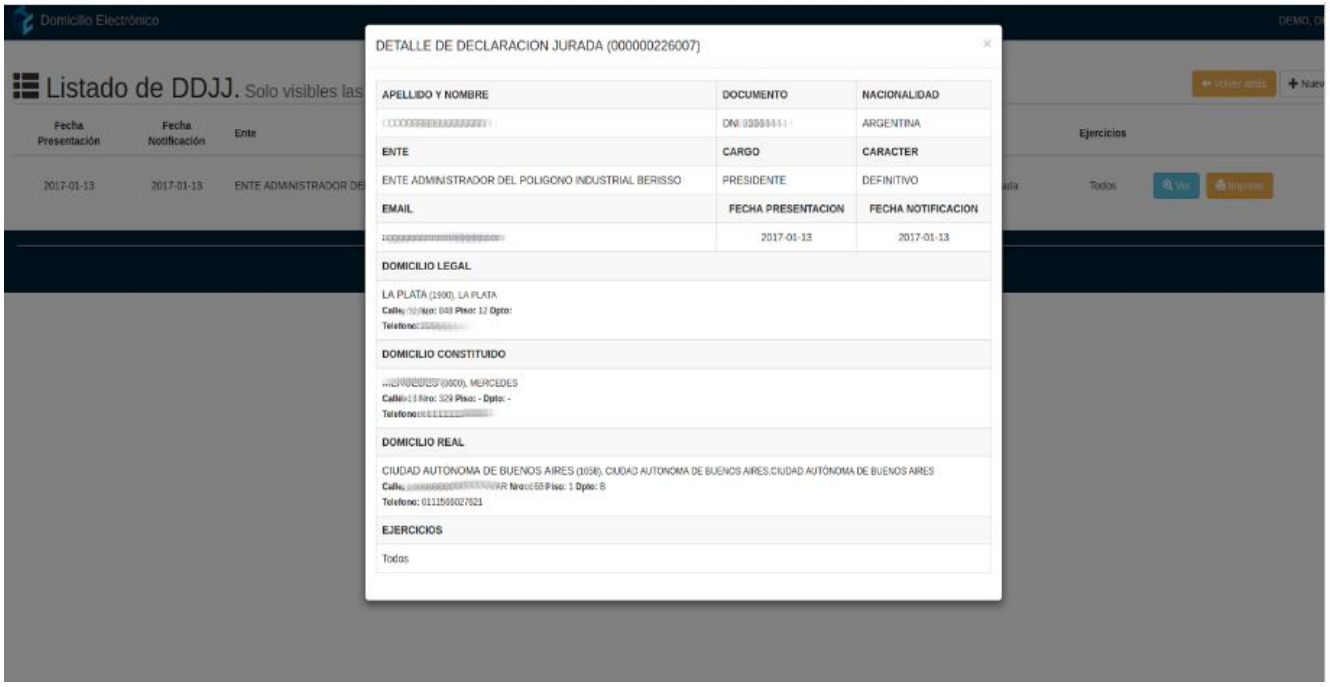


Fig. 5.11. Detalle de la DJ Web

4.3.3. Mesa de ayuda

Servicio creado para facilitar la comunicación e interacción con los usuarios de Notificación Electrónica. Se pueden canalizar, a través de la misma, consultas, reclamos y sugerencias.
Los medios disponibles para brindar ayuda al usuario son:

- Preguntas Frecuentes: Listado de preguntas elaboradas por funcionarios del HTC (Fig.5.12).

Fig.5.12.Preguntas frecuentes

- Consultas Web: Formulario web que permite al usuario expresar sus dudas. Las mismas serán respondidas por correo electrónico. Dicho formulario está compuesto de 3 pasos:

  - Información de Contacto (Fig.5.13).
  - Consulta (Fig.5.14).
  - Confirmar Información (Fig.5.15).

- Si fuera necesario se brindarán respuestas a las dudas mediante atención telefónica.

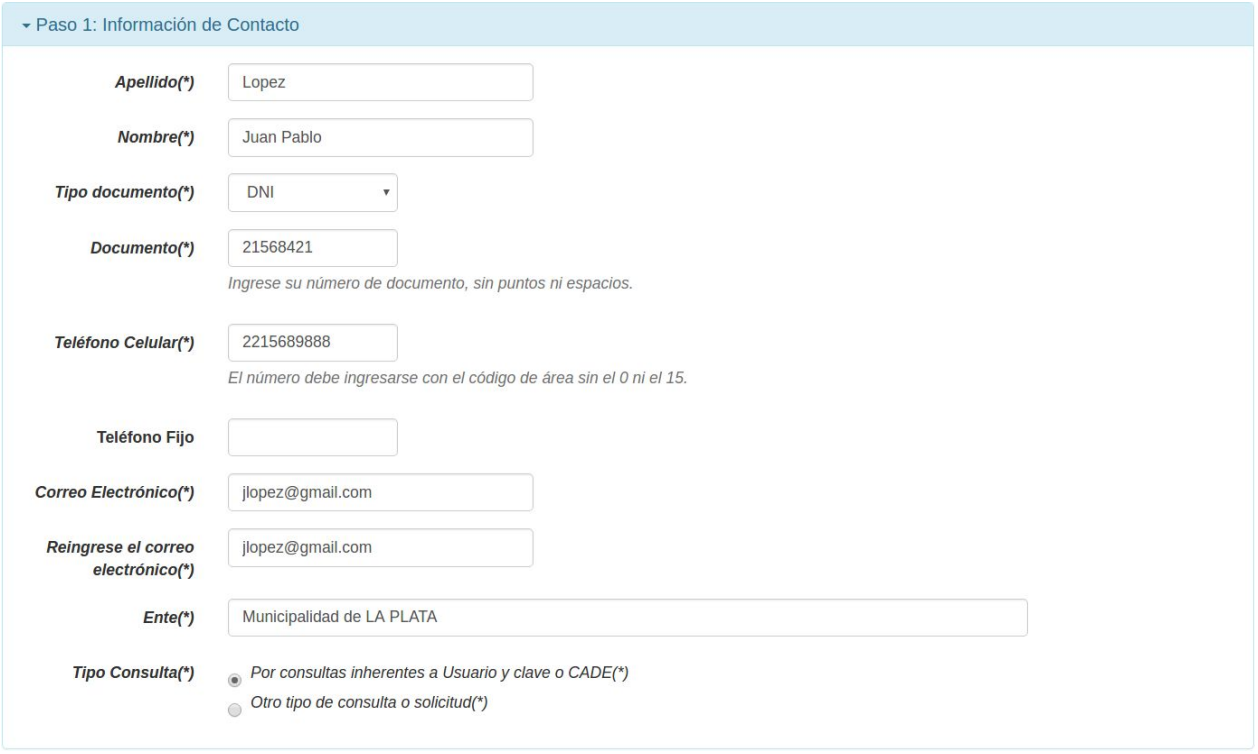


Fig.5.13. Paso 1: Información de Contacto

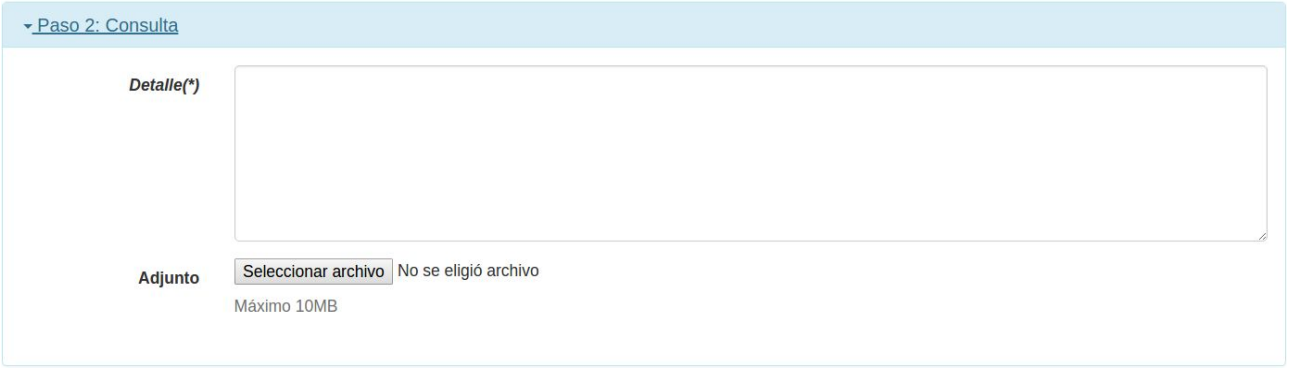


Fig.5.14. Paso 2: Consulta

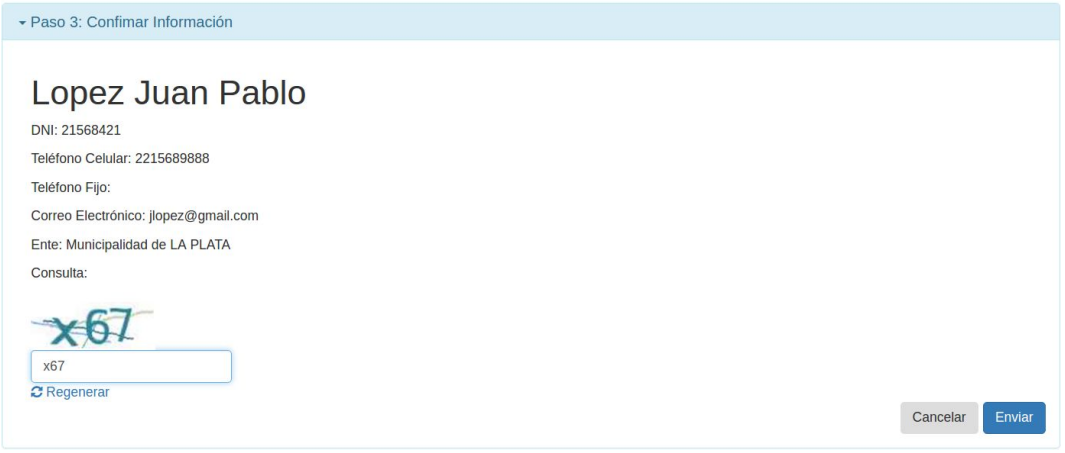


Fig.5.15. Paso 3: Confirmar Información

Capítulo 5

5. Segno

5.1. Investigación

En principio se investigaron distintos firmadores *open-source* que circulan por la red.
Luego de analizar las distintas propuestas encontradas se hallaron los siguientes problemas:

- Soluciones stand-alone.

- Uso de applets.

Las soluciones de tipo standalone o Desktop no permiten la integración con el resto de las aplicaciones web utilizadas en el organismo. El usuario debe instalar el software en forma local, descargar un documento pdf a firmar, para luego subirlo a la aplicación web, lo cual genera un circuito engorroso a fines de facilitar el proceso, de por sí, *muy complejo.*
La mayoría de los firmadores basados en tecnología web se encuentran desarrollados con applets de java, la cual será *descontinuada en el futuro cercano*.

Las razones por las que se descartó el uso de esta tecnología son las siguientes:

- Requiere un plugin de Java a instalarse en el navegador y Oracle ya anunció que abandonará este desarrollo a partir de la versión 9 de Java.

- Sun no ha creado una implementación del plug-in para los procesadores de 64 bits.

- Un applet podría exigir una versión específica del JRE.

- Puede tener vulnerabilidades que permiten ejecutar código malintencionado.

A continuación se mencionan los *firmadores* analizados:

Xolido Sign

- Xolido®Sign Desktop [45] es un producto gratuito, universal, estable, altamente probado, con soporte gratuito y continuidad.

- Permite firmar una gran variedad de documentos como PDF, Word, Excel, JPEG, vídeos, PowerPoint, archivos txt, imágenes, diseños vectoriales.

- Posee soporte para sellado digital en el tiempo (Timestamping).

- Otra característica es que permite firmar por lotes.

- La razón principal por la que se descartó dicho software para utilizar en el organismo es que sólo posee la versión Desktop de manera gratuita.

I-SIS Firmador Digital

Otro de los firmadores estudiados fue I-SIS Firmador Digital [46]. Dicho software en su versión gratuita posee las siguientes características:

- Firma de PDF.
- Visor de documentos.
- Posibilidad de ubicar la firma.
- Firma visible.
- Ubicación automática.
- Validación de firma.
- Envío de documentos por mail.
- Compatibilidad con estándares y dispositivos criptográficos.
- Verificación de firma contra CRL.
- Consulta OCSP al verificar firmas.
- Integración con dispositivos PKCS#11, CryptoAPI de Windows (Repositorio de Certificados de Windows), archivos P12, DER, PEM.
- Incorporación de datos del firmante, obtenidos de su Certificado X509 v3, en la estampa visible de la firma.

A diferencia de Xolido Sign, I-SIS Firmador digital no permite la firma por lotes. Sin embargo ambos firmadores poseen versiones gratuitas en modo Desktop.

Applet Firmador Digital de PDF

El applet firmador de PDF es un desarrollo basado en el firmador pdf de la ONTI. Del mismo se pueden destacar las siguientes funcionalidades:

- Funciona con un token-usb o keystore del navegador/SO.
- Permite firmar un único o múltiples documentos individuales.

- Valida la vigencia de certificados y OCSP (chequeo certificados revocados). Chequeo cadena de certificados (trusted-certificates).

- Visualización online del documento (si lo permite navegador). Descarga/apertura en SO.

- Integración sencilla con aplicaciones.

Dicho firmador cumplía con la mayoría de los requisitos para ser utilizado en el ámbito provincial, además de estar avalado por la ONTI, pero *está implementado con Applets de Java* con los problemas que esta tecnología implica.

Cuadro comparativo de los firmadores analizados

	Xolido Sign	**I-SIS Firmador digital**	**Firmador Digital ONTI**
Aplicación Desktop	X	X	
Ubicación personalizada de la estampa		X	
Verificación contra CRL	X	X	X
Verificación contra OSCP		X	X
Uso de Applets			X

HSM

Un HSM [47] (Hardware Security Module) es un dispositivo de seguridad que genera, almacena y protege claves criptográficas (PKI). Si bien existen diversos software que generan módulos de certificación, cabe destacar que HSM proveen mayor nivel de seguridad.

Los HSM permiten generar claves para certificados digitales de clave pública y admiten rutinas con un grado de aleatoriedad muy alto, así como almacenar las contraseñas de acceso a determinados certificados.

Evaluación del uso de HSM

Otro escenario evaluado fue con la interacción de un HSM. En este caso la clave privada del usuario se guarda en una partición del HSM, la cual es accedida mediante un pin que conoce el mismo usuario. La aplicación web interactúa directamente con el HSM mediante una conexión segura.
El inconveniente de este escenario es que se imposibilita al usuario de poseer un token donde se guarde la clave privada.
Otra de las razones por las que se decidió no desarrollar esta solución se debe a que la ONTI (Oficina Nacional de Tecnologías de la Información) no contaba con un proceso formal para la instalación de certificados en este tipo de dispositivos.

Conclusiones

Luego de un análisis exhaustivo de los firmadores anteriormente mencionados se determinó comenzar un desarrollo propio de un firmador que posea los mejores aspectos del software visto. A fin de poder satisfacer los requerimientos relevados en el organismo, se necesitaba que el firmador interactúe con los sistemas ya desarrollados, y su inclusión sea lo menos costosa posible. Por ese motivo se llevó a cabo **Segno**, *un firmador capaz de interactuar con cualquier sistema web, siguiendo un mecanismo de comunicación establecido para firmar documentos PDF.*

Segno combina una serie de características que, en conjunto, no son provistas por los firmadores analizados anteriormente. A continuación se enumeran las mismas:

- ✓ Unificación del uso del firmador en diferentes aplicaciones
- ✓ Uso de tecnologías open-source
- ✓ Actualización automática del firmador.
- ✓ Bajo mantenimiento del firmador.

Cabe destacar que la implementación de un desarrollo propio permite el control y evolución del software con la consecuente reducción de los riesgos asociados a la gestión del cambio.

5.2 Desarrollo

Arquitectura

Segno está desarrollado siguiendo el modelo Cliente/Servidor (Fig.6.1) , en donde las tareas se reparten entre el proveedor de recursos o servicios, denominados servidor y el demandante llamado cliente.

En este caso el rol de cliente es asumido por Segno, el cual es instalado en cada equipo y actúa de wrapper para varias aplicaciones del HTC.
El servidor está representado por las aplicaciones que proveen los documentos para firmar.
La comunicación entre la aplicación cliente y el servidor se realiza mediante servicios RESTful utilizando JSON como formato de datos de transferencia. Además, en dicha comunicación, se utiliza un token con el objetivo de autenticar cada requerimiento del cliente al servidor.

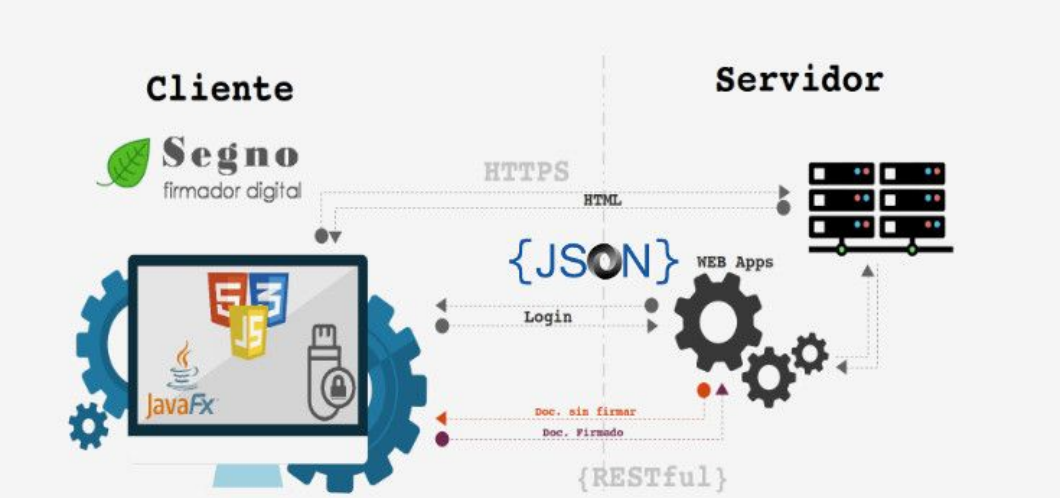


Fig. 6.1. Arquitectura

Tecnologías y paradigmas utilizados

La selección de herramientas a utilizar en todo desarrollo es una decisión importante, se realiza en etapas tempranas y se determina de acuerdo a diferentes aspectos, como la idiosincrasia del organismo, conocimientos de los desarrolladores, puntos fuertes de cada tecnología, etc.
A continuación se detallan las tecnologías usadas tanto del lado del cliente como del servidor.

Cliente

Segno está desarrollado utilizando JavaFX, la cual es una familia de productos y tecnologías para la creación de Rich Internet Applications (RIAs) permitiendo aplicaciones con experiencias visuales que resulten atractivas.
Además usa la librería iText para la manipulación de archivos PDF y Bouncy Castle Crypto para administrar el uso de algoritmos criptográficos.

Fig.6.2. Tecnologías del lado Cliente

Servidor

La construcción de la infraestructura tecnológica del HTC (Fig.6.3) tuvo como filosofía la elección de componentes para cuyo uso no es necesario el pago de licencias.
En este marco dicha infraestructura está soportada en “VMWare” [48]. El servidor web está compuesto por “Debian” [49] como sistema operativo y el servicio web, para el acceso a las aplicaciones del HTC, está soportado por “Apache” [50] al que se le ha incorporado el firewall de aplicación “ModSecurity”.
El acceso a las aplicaciones del HTC se realiza mediante la intranet del organismo y está soportada por un sistema propio de acceso unificado de usuarios.
Para autenticar a los usuarios, el mismo usa un servidor “LDAP” y un administrador de roles y permisos para las aplicaciones.
La gestión de proyectos informáticos del HTC es llevada a cabo mediante “REDMINE”, herramienta de código abierto para la gestión de proyectos . Dicha herramienta está soportada por un servidor web “Mongrel” con soporte para “Ruby”.
Los proyectos de software del HTC están desarrollados bajo el framework de desarrollo Symfony 2 y se utiliza “SVN” para el versionado de los mismos. El sistema de gestión de base de datos (SGBD) utilizado es “MySql” [51].

6.3. Tecnologías del lado del Servidor

Aplicaciones

Del lado del servidor, se encuentran las aplicaciones que proveen a Segno de los documentos PDF a firmar. Actualmente, dichas aplicaciones son:

- Holos: Sistema utilizado para gestionar paquetes que contienen los documentos a ser firmados. Además posee un módulo para el envìo de los mismos al DE correspondiente.

- Notificaciones: Sistema que permite la generación de notas y cédulas de notificación a los alcanzados de Estudios de Cuentas. Se basa en tecnología de generación de plantillas dinámicas de documentos y se vincula con otros sistemas del HTC.

El acceso a cada una de los sistemas se realiza a través de la intranet (Fig. 6.4) del organismo bajo el criterio de “usuario único”, el cual unifica el acceso a todos las aplicaciones.

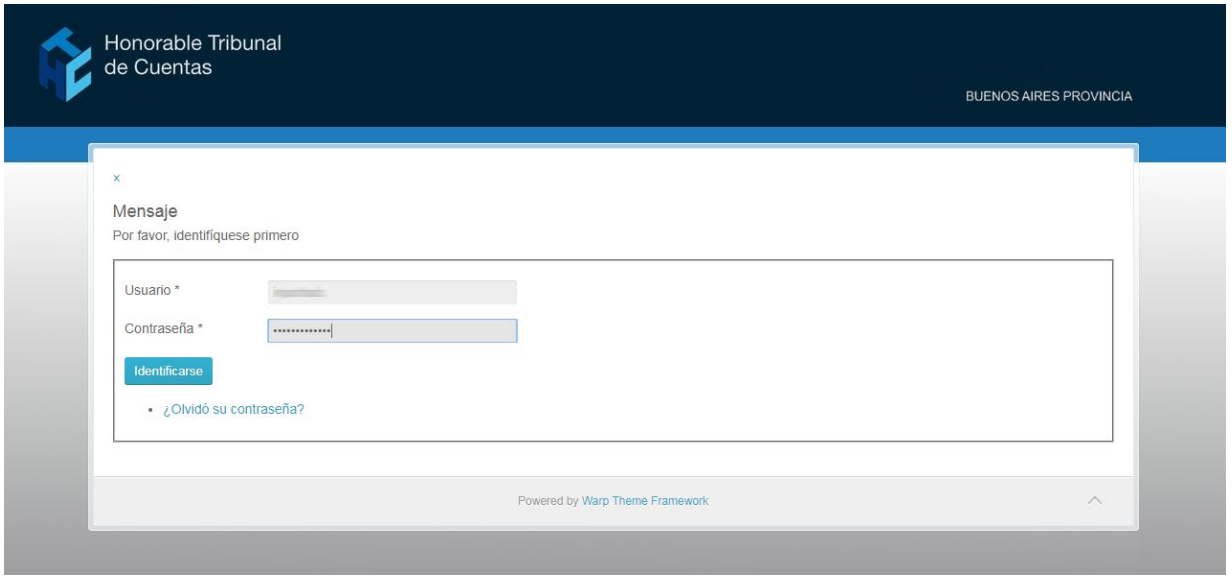


Fig.6.4. Acceso a intranet del HTC

Holos

En la figura 6.5. se visualiza la pantalla principal del sistema Holos, en dónde se gestionan los documentos que luego serán firmados digitalmente por Segno y posteriormente enviados al domicilio electrónico de los responsables.
De cada documento se pueden observar los siguientes datos:

- Fecha en la que se cargó el documento.
- Tipo de Documento, el cual puede ser: Comunicación simple, Fallo,Traslado 27, y Traslado 39.
- Unidad Documental al que pertenece el documento.
- Estado. Un documento puede encontrarse en uno de los siguientes estados:
    - ***Cargado***: Documento cargado en el sistema sin ningún visado.
    - ***Visado Previo***: Primer visado realizado por un responsable del HTC.
    - **Visado**: Visado definitivo por un responsable del HTC diferente al que realizó el visado previo.
    - ***Listo para enviar***: El documento se encuentra firmado digitalmente por lo que puede ser enviado al DE del cuentadante.
    - ***Enviado incompleto***: En el caso de que uno o más cuentadantes no posean el DE creado, será un envío incompleto.
    - ***Enviado completo***: Las notificaciones fueron enviadas a la totalidad de los responsables.

- ***Notificado***: Los cuentadantes se han dado por notificados a través de su DE.

➢ Anexo: Cantidad de archivos adjuntos al documento original.

➢ Responsables: Cantidad de cuentadantes que son alcanzados por el documento.

➢ Auditoría: Información sobre los usuarios que crearon, revisaron y modificaron el documento.

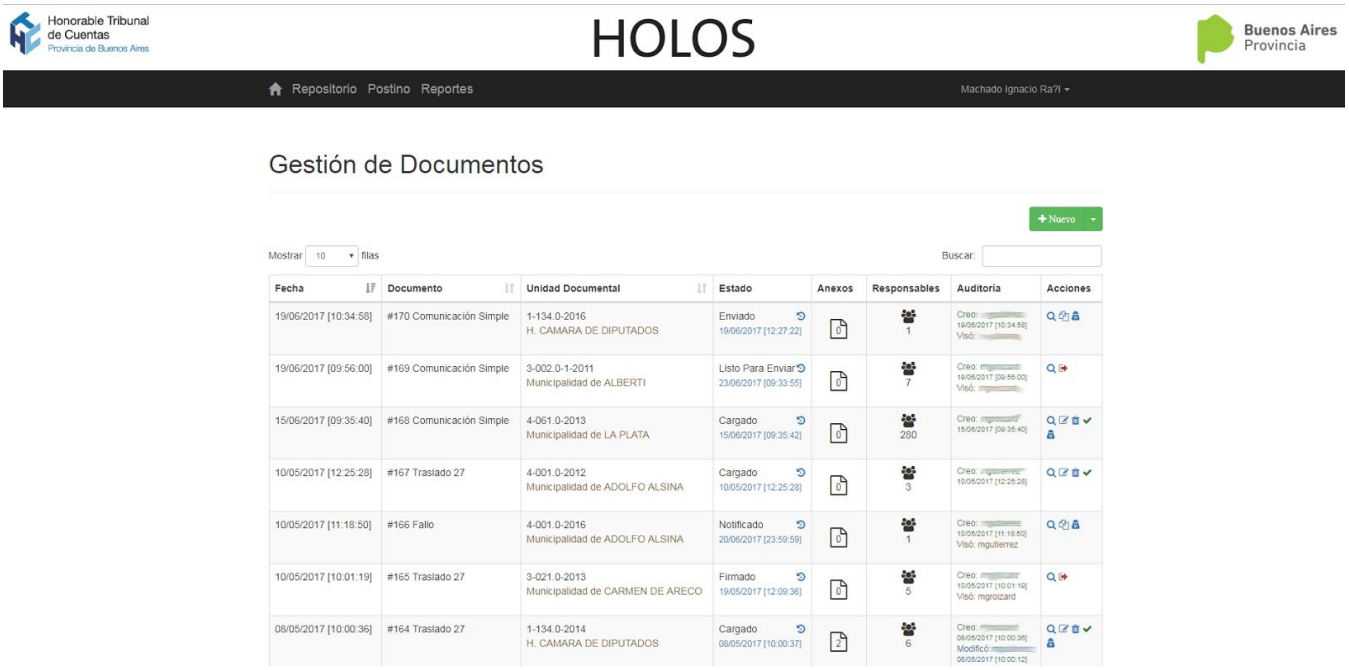


Fig.6.5. Pantalla principal de Holos

Para cargar un nuevo documento es necesario acceder por medio del botón “Nuevo” y seleccionar el tipo de documento deseado.
En la figura 6.6 se visualiza el formulario para la carga de nuevos documentos.

Fig.6.6. Carga de un Traslado 27

Una vez que el documento fue visado en las 2 instancias, se visualiza en Segno para poder ser firmado digitalmente.
Posteriormente accediendo al menú “Postino” (Fig. 6.7) de Holos se dispone el botón “Enviar” , para hacer llegar los documentos correspondientes al DE de los cuentadantes.

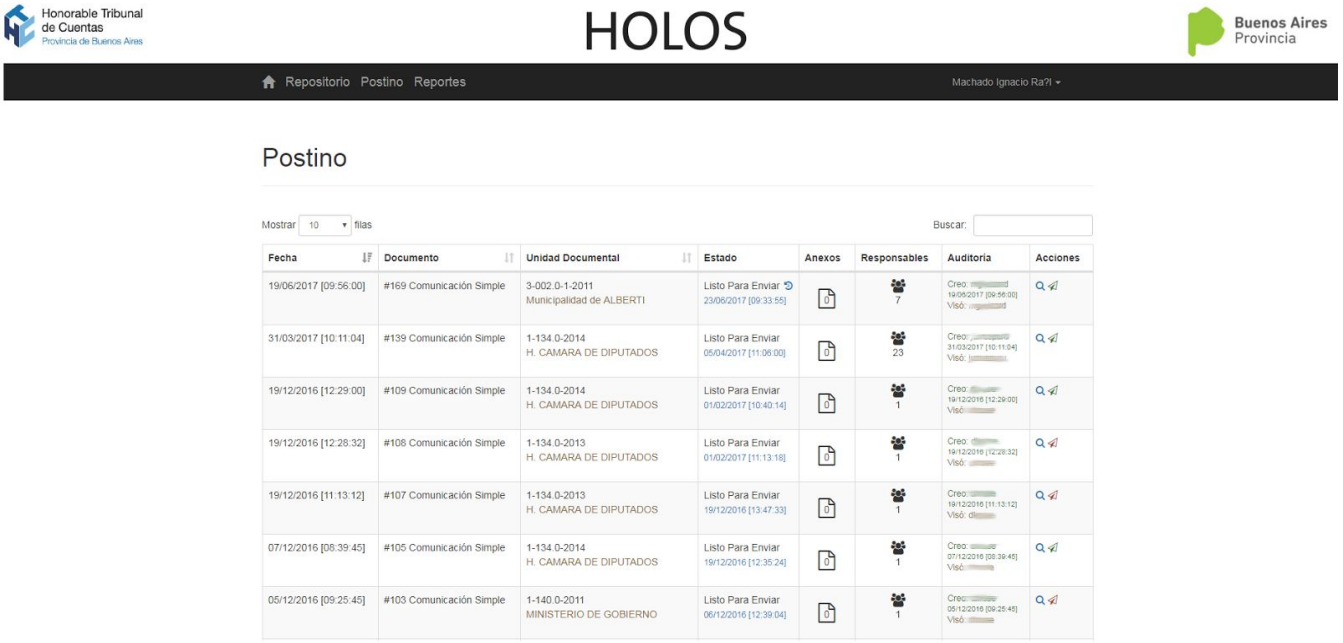


Fig.6.7. Envío de documentos

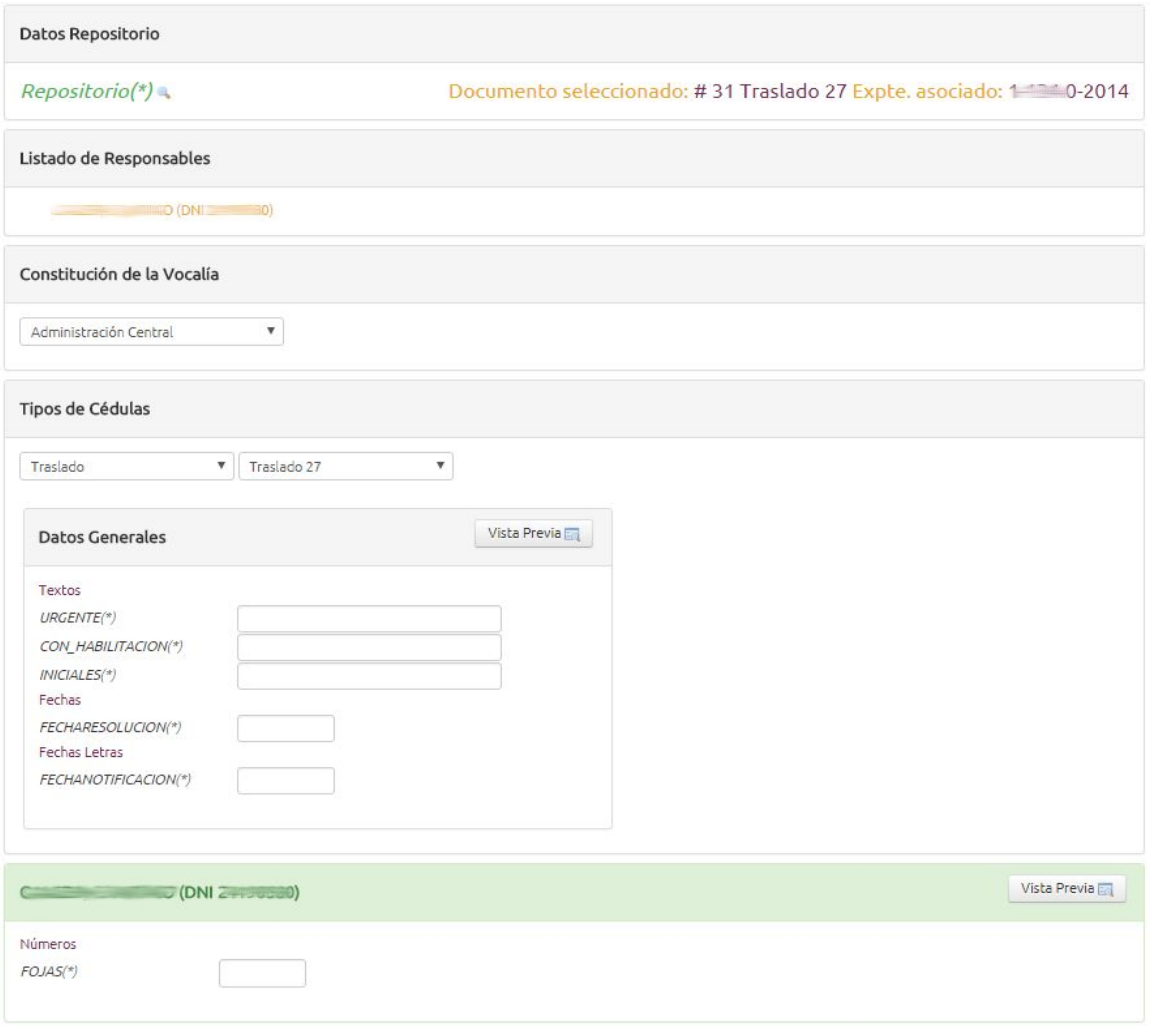
Notificaciones

En la pantalla principal de Notificaciones (Fig.6.8) se visualiza el acceso al módulo de “Cédulas digitales”, las cuales son utilizadas en el circuito de notificación electrónica.

Fig. 6.8. Pantalla principal de Notificaciones

En el módulo de cédulas digitales puede observarse el listado (Fig.6.9) de las cédulas cargadas hasta el momento.
Del mismo modo, Notificaciones permite la carga de nuevas cédulas digitales a través del formulario ilustrado en la Fig.6.10.

6.9. Listado de cédulas digitales



6.10. Carga de cédula digital

5.3. Descripción Funcional

Instalación

Para utilizar Segno es necesario instalarlo del mismo en cada equipo donde se ejecutará. Dicho proceso por convención se realiza de la siguiente manera:

- Se crea una nueva carpeta (C:\Segno, por ejemplo).
- Se coloca el .jar (Segno.jar) en dicha carpeta.
- Para facilitar el acceso al usuario se crea un acceso directo en el escritorio.

- La primera vez que se ejecute, se descargará todo lo necesario para poder firmar correctamente.

Acceso

Para iniciar Segno, es necesario ejecutar dicha aplicación e iniciar sesión con el usuario y contraseña utilizado en todas las aplicaciones del HTC (Fig. 6.11).

Fig.6.11.Login de Segno

Una vez ingresado a Segno, se visualizan los tipos de documentos que se pueden firmar actualmente: Notificaciones y documentos de repositorio. Ambos son provistos por diferentes aplicaciones, el sistema *Notificaciones V3* para el primer caso y *Holos* para el segundo. Esto puede observarse en la fig. 6.12.

Fig. 6.12. Selección de tipos de documentos a firmar

Dentro de los documentos de repositorio provistos por Holos podemos distinguir:

- Fallos.
- Traslados 27.

- Traslados 39.

- Comunicaciones Simples.

Dichos documentos son generados en las vocalías del HTC, posteriormente enviados por otro sistema llamado Postino, el cual se encargará de enviar las notificaciones correspondientes al domicilio electrónico de los cuentadantes.
Como puede observarse en la Fig. 6.13. se visualizan todos los documentos que el usuario posee para firmar. Cada fila mostrada informa los siguientes datos del documento:

- **Fecha** desde que está disponible para firmar.

- El tipo de **documento** a firmar junto con el número de paquete indicado con el carácter **#** .

- La **Unidad Documental** (Nº de expediente) junto con el organismo al que pertenece el cuentadante para ese ejercicio.

- La cantidad de documentos **anexos** que posee ese documento y que también serán firmados digitalmente.

- Información de **auditoría** para conocer quien creó y visó dicho documento.

- Además como acción se permite visualizar los documentos que van a ser firmados (Fig. 6.14).

Fig. 6.13. Bandeja principal de documentos de repositorio

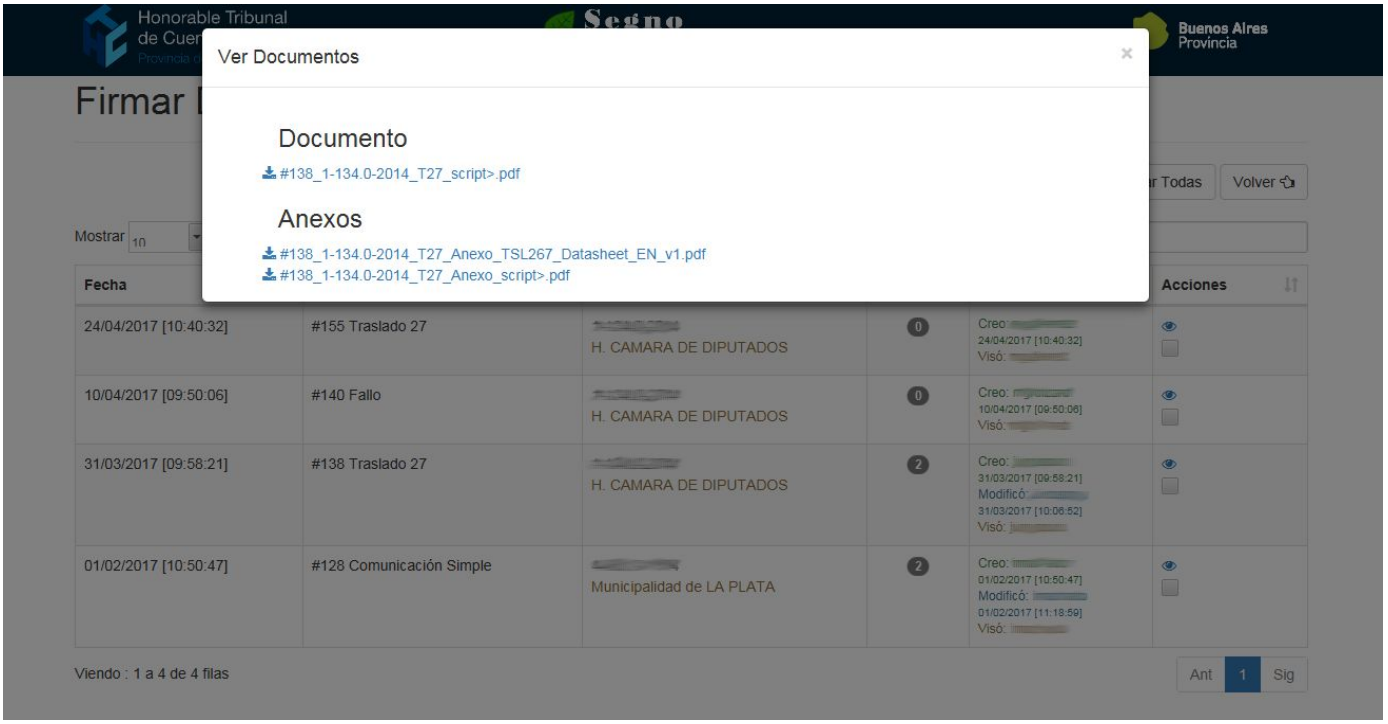


Fig. 6.14. Visor de documentos

Volviendo a la Fig. 6.12 el usuario puede seleccionar la opción “Firmar Notificaciones”. Seguidamente se visualizan los tipos de documento provistos por el sistema Notificaciones V2. Actualmente provee Cédulas y Notas (Fig. 6.15). Dichos documentos se generan a partir de los traslados firmados en la sección de Documentos de repositorio.
Las cédulas a diferencia de los Traslados, fallos y comunicaciones simples suelen ser firmadas por los responsables de la secretaría de actuaciones y procedimientos del HTC.

Fig.6.15. Documentos provistos por Notificaciones V2

Ambos botones dirigen al usuario a una bandeja (Fig.6.16) que contiene la siguiente información:

- **Fecha** desde que el documento está listo para firmar.
- La **Unidad Documental** (Nº de expediente) junto con el organismo al que pertenece el cuentadante para ese ejercicio.
- **Tipo de cédula.** Actualmente sólo se firma cédulas de traslados.
- **Modelo de cédula.** Puede ser 27 o 39, dependiendo del tipo de traslado.
- El número de **paquete** al que pertenece.
- La **cantidad de cédulas.**
- El **sector** que creó la cédula.

Fig.6.16. Cédulas provistas por Notificaciones V2.

Funcionalidades

A continuación se mencionan las funcionalidades que proporciona *Segno*:

- ✓ Firma de documentos PDF y protección de los mismos contra modificaciones y copiado de información.
- ✓ Integración con dispositivos PKCS#11.
- ✓ Soporte para múltiples firmas.
- ✓ Incorporación de datos del firmante, obtenidos de su Certificado en la estampa visible de la firma.
- ✓ Imagen de firma personalizada.
- ✓ Soporte para la inclusión de Sello de Tiempo incrustado.
- ✓ Visor de documentos

Validaciones

Segno realiza diversas validaciones para lograr que la firma sea lícita y que también constituya un sistema seguro. Dichas validaciones son:

- ✓ **Certificado firmante contra la CRL:** se verifica que el certificado instalado en el token del usuario no se encuentre en la lista de revocación de certificados provistas por la ONTI (Fig 6.17). De ser así, Segno lo informará por pantalla y el usuario no podrá firmar ningún documento si mantiene esta condición(Fig.6.18).

- ✓ **Caducidad del certificado firmante:** los certificados provistos poseen una fecha de caducidad, por lo que el sistema valida que nos encontremos en una fecha válida antes de firmar (Fig.6.19).

- ✓ **CUIT/CUIL del certificado y el usuario logueado en el sistema:** esta validación se realiza para que solamente pueda firmar el titular del token con su usuario utilizado para acceder a las aplicaciones del HTC (Fig.6.20).

```
public  boolean verifyCertificateCRLs(X509Certificate cert) throws SegnoException,
CertificateParsingException, IOException, CertificateException, CRLException
       {
       try {
            List<String> crlDistPoints = getCrlDistributionPoints(cert);
            for (String crlDP : crlDistPoints) {
                logger.info("Descargando CRL");
                X509CRL crl = downloadCRLFromWeb(crlDP);
                logger.info("Verificando CRL");
                if (crl.isRevoked(cert)) {
                   DateFormat dateFormat = new     SimpleDateFormat("yyyy/MM/dd HH:mm:ss");
                   Date date = new Date();
                   logger.error(dateFormat.format(date) + " - Certificado revocado " );
                   throw new SegnoException("1");
                 }
              }

         } catch (IOException ex) {
              logger.error("ERROR:::: " + ex.getMessage());
              throw new SegnoException("2");
              // NO SE PUDO COMUNICAR CON LA CRL
              }
              return true;
       }
```

Fig. 6.17. Método que verifica si el certificado se encuentra revocado

Fig.6.18. Certificado revocado

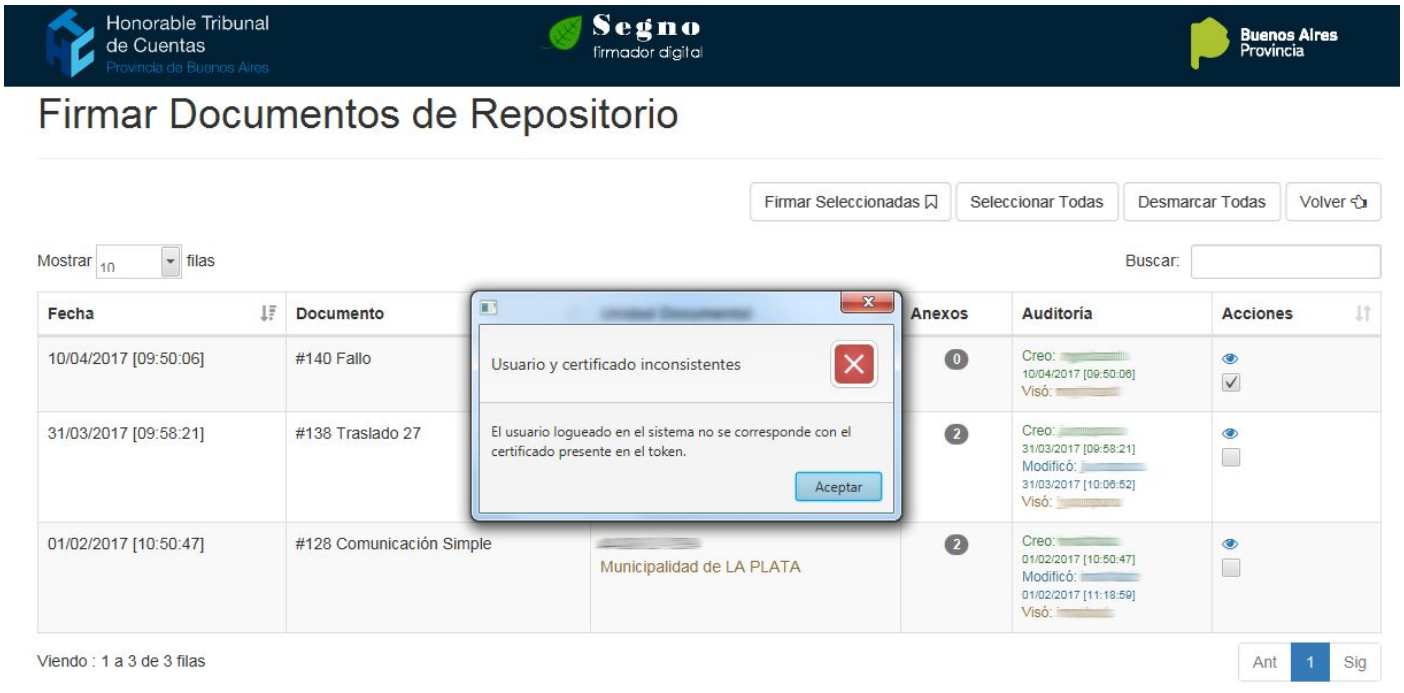


Fig.6.19. Usuario y certificado inconsistentes

Fig.6.20. Certificado vencido

Manejo de errores

Como todo sistema, Segno posee un manejo de errores en tiempo de ejecución. A continuación se mencionan aquellos que se consideran más importantes:

- Token no conectado: como su nombre lo indica, el dispositivo para firmar no se encuentra conectado en el puerto USB correspondiente o no fue reconocido por el sistema (Fig. 6.21)

- Pin incorrecto: el pin ingresado no es correcto, sin embargo se puede volver a intentar. Existe un límite de 15 intentos, pasado ese número se bloqueará el dispositivo y el usuario deberá realizar el trámite correspondiente nuevamente para obtener el nuevo certificado (Fig.6.22).

- Paquete ya firmado: puede ocurrir que una vez que se visualizaron los documentos a firmar, alguno de ellos sea firmado por otro usuario, sucediendo así un error por intentar firmar dos veces el mismo documento (Fig. 6.23).

Fig.6.21. Token no conectado

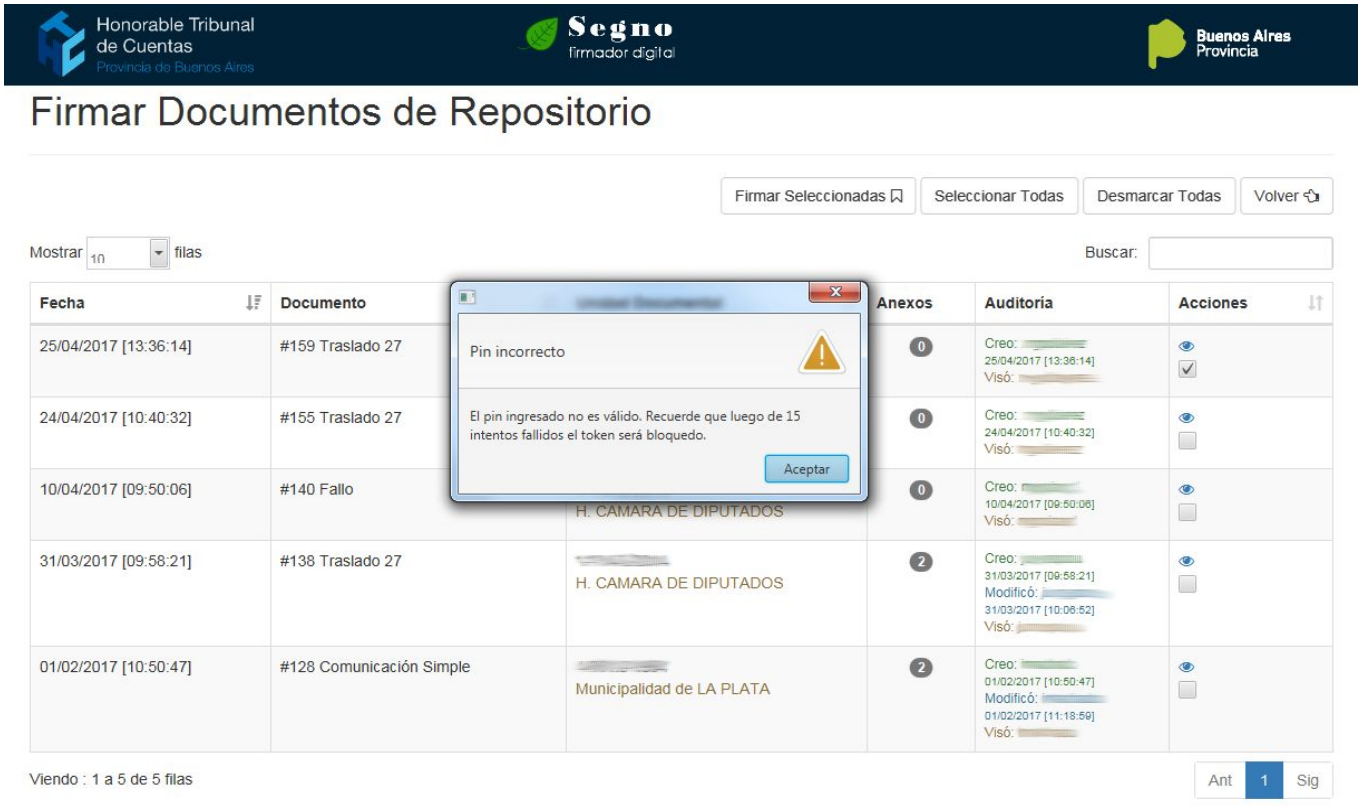


Fig.6.22. Pin incorrecto

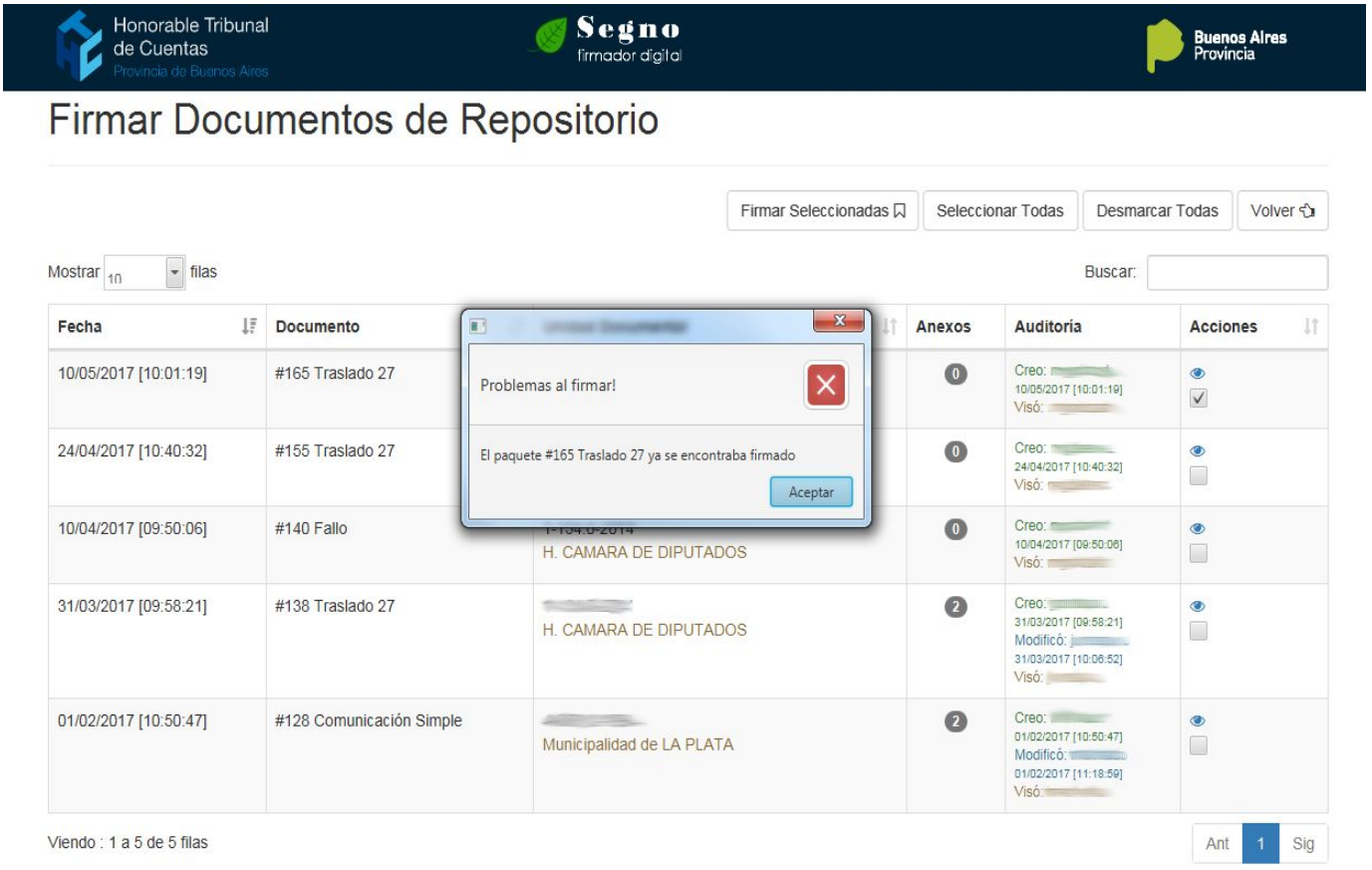


Fig.6.23. Paquete ya firmado

Visualización de la firma

Para visualizar correctamente la firma es necesario contar con los certificados provistos por la ONTI.
Dichos certificados pueden *descargarse desde el sitio* https://www.argentina.gob.ar/firmadigital.(Fig. 6.24). De esta manera se obtiene el Certificado de Autoridad certificante y el Certificado raíz.
Para instalar ambos certificados basta con *hacer click derecho sobre el certificado, "Instalar Certificado".*
Por último, debe configurarse el Acrobat Reader. Para ello ir a *Edición->Preferencias, seguidamente acceder a Firmas->Verificación, botón más (*como puede observarse en la Fig.6.25).
Para finalizar la configuración se debe seleccionar la opción *"Validando Firmas"* (como muestra la Fig.6.26 y aceptar).

Fig.6.24. Sitio para descargar los certificados (28/05/2017)

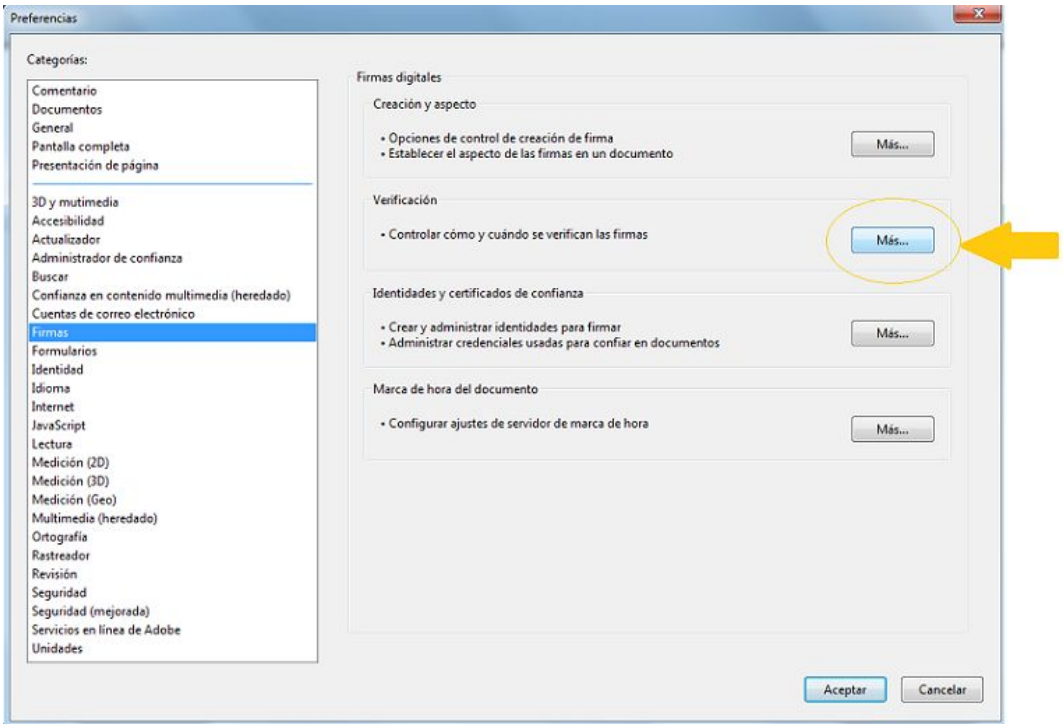


Fig.6.25. 1er Paso Configuración de Acrobat Reader

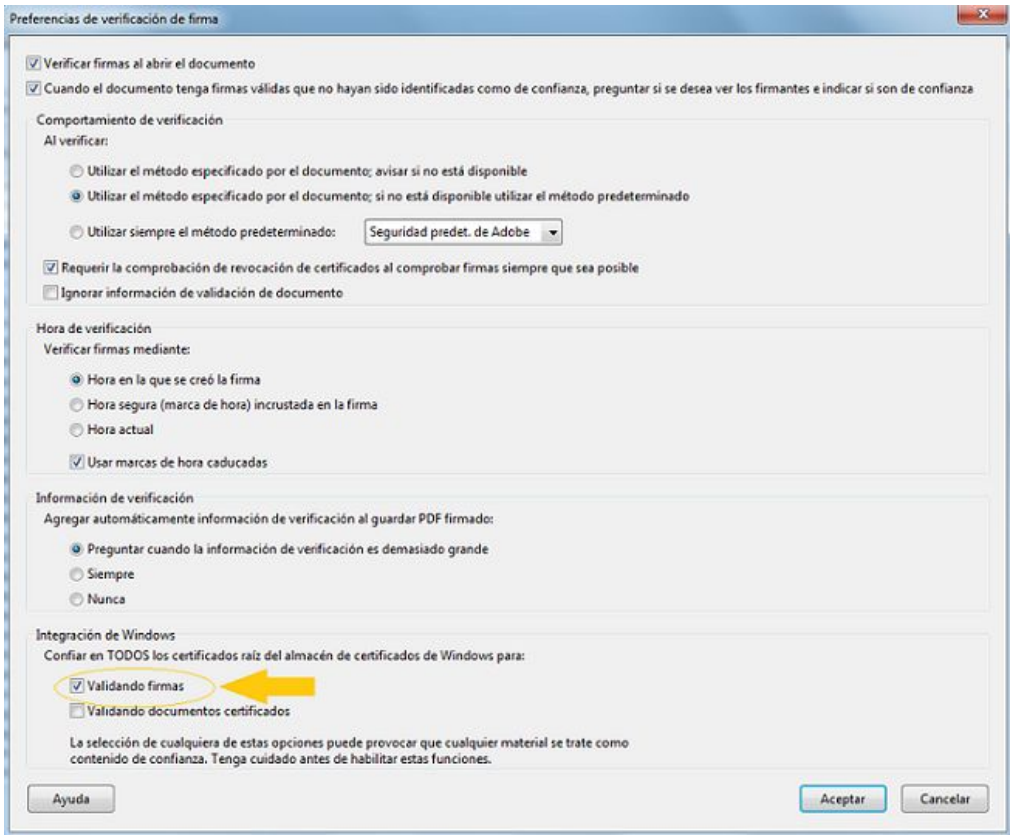


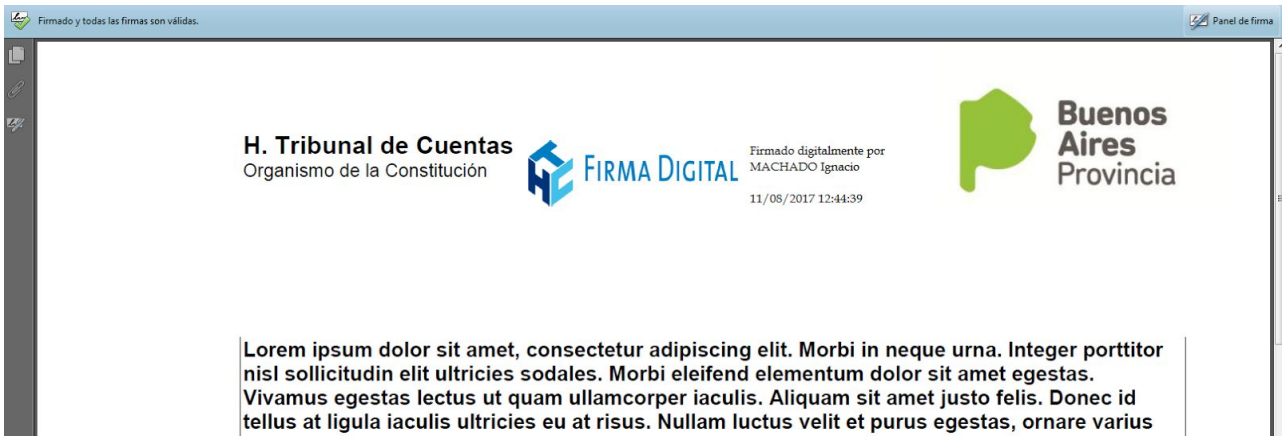
Fig. 6.26. Último paso de configuración de Acrobat Reader

Otra de las cuestiones que se tuvo en cuenta fue la imagen con la que se percibiría la firma. El primer diseño desarrollado fue la Fig.6.27. Posteriormente se desarrolló un diseño más personalizado para el HTC (Fig. 6.28).

Fig. 6.27. Primer diseño de la estampa

Fig.6.28. Diseño definitivo de la estampa

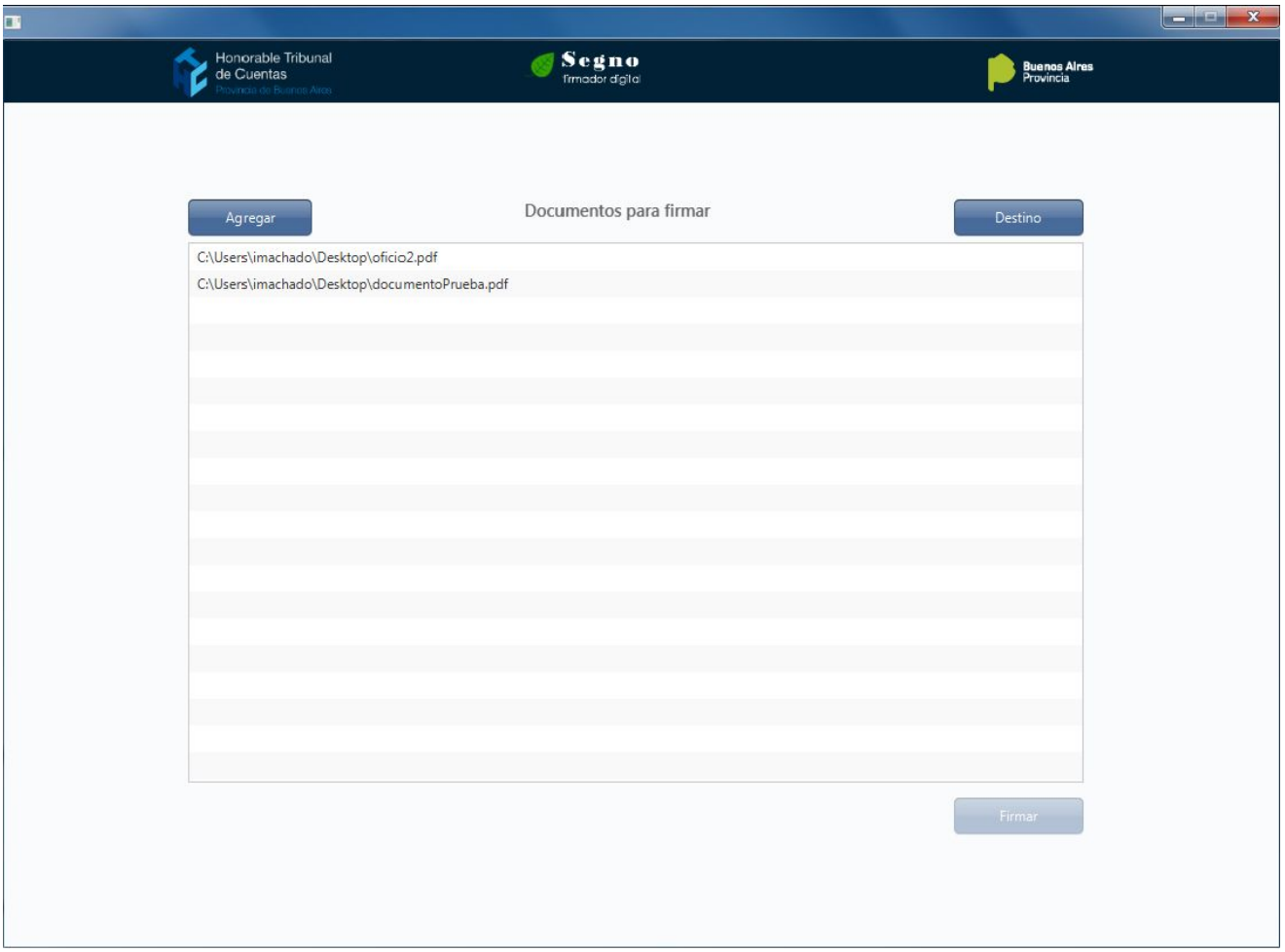
Finalmente un documento firmado digitalmente por Segno se visualiza como se muestra en la Fig.6.29



6.29. Visualización de la firma de un documento

5.4. ***DSegno***, versión de escritorio

Luego de la implementación de Segno, se planteó la posibilidad de firmar documentos digitalmente sin la necesidad de incorporar los documentos al circuito de notificación electrónica. Es decir, documentos que no se encuentren en *Holos*, *Notificaciones* o cualquier aplicación web del HTC. Para ello se realizó una investigación de las posibilidades para enfrentar dicha problemática. La solución que se determinó fue utilizar las bases de Segno e implementar un nuevo firmador únicamente de escritorio. De ahí nace ***DSegno***, un firmador digital stand-alone, con los mismos conceptos que ya se habían desarrollado permitiendo reutilización de código sin “reinventar la rueda”.
Se propuso una interfaz muy sencilla (Fig.6.30), donde se dispone una bandeja que muestra los archivos que se van a firmar.



6.30. Pantalla principal de DSegno

La novedad más importante de esta versión es la posibilidad de elegir la ubicación que tendrá la estampa de la firma en cada documento (Ver Fig.6.31). Haciendo doble click sobre el archivo deseado, se puede observar la vista previa del documento permitiendo seleccionar donde quedará ubicada la estampa.

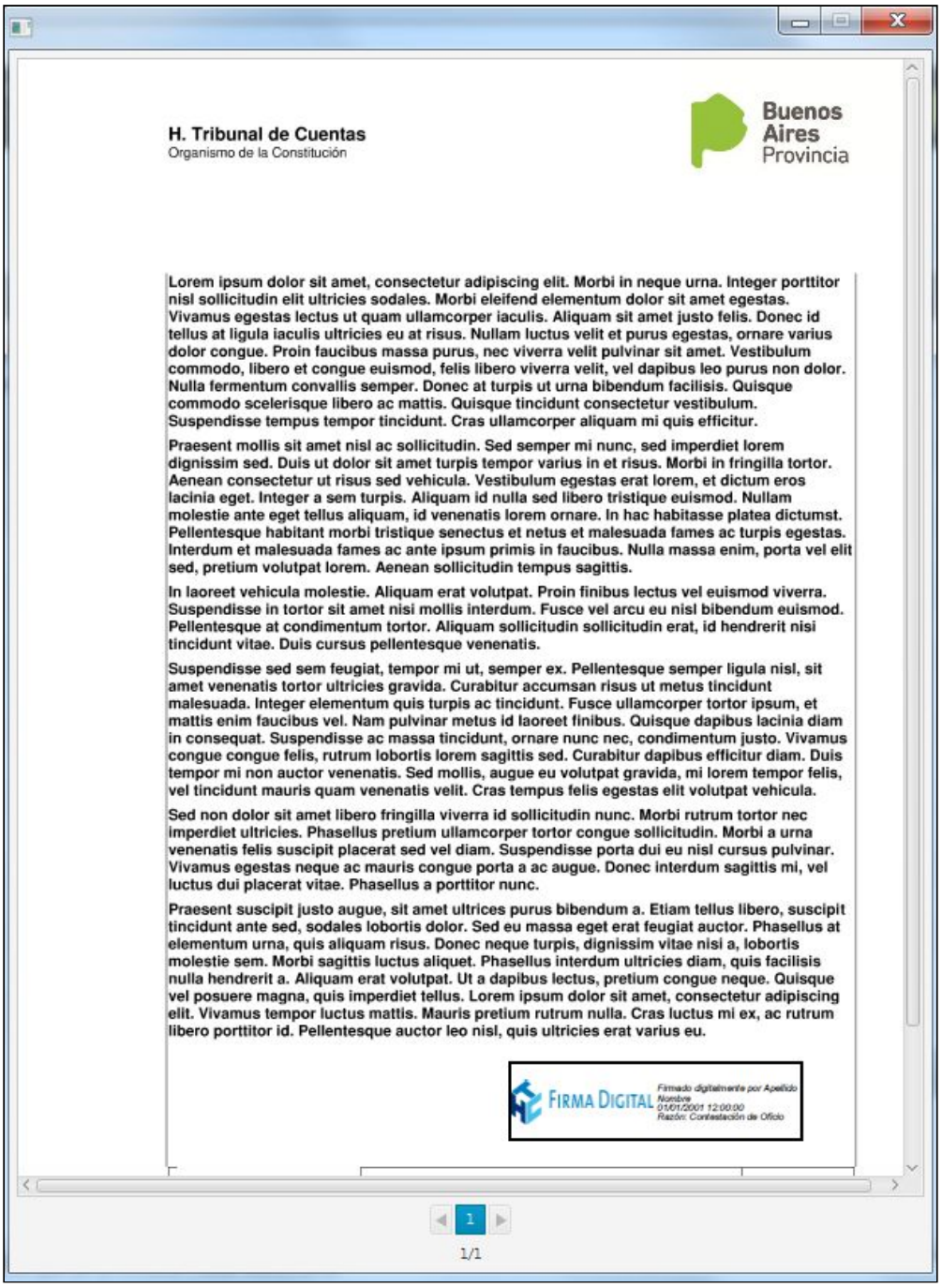


Fig.6.31. Ubicación de la estampa

Una vez que se ha seleccionado la posición de la firma (si no se define, existe una por defecto), se debe indicar la carpeta destino donde se almacenará el archivo firmado y por último se necesita presionar el botón Firmar, indicando el pin del token.

Capítulo 6

6. Resultados, Conclusiones y Trabajos a Futuro

6.1 Resultados

Del análisis de los datos, se obtuvo que al mes de Julio de 2017 se habían firmado 126 fallos, 1390 cédulas de notificación, 181 informes de traslado y 267 comunicaciones simples.
Para el mismo mes se han efectuado 1019 notificaciones a los cuentadantes correspondientes. Las mismas se detallan por tipo de documento en el siguiente cuadro:

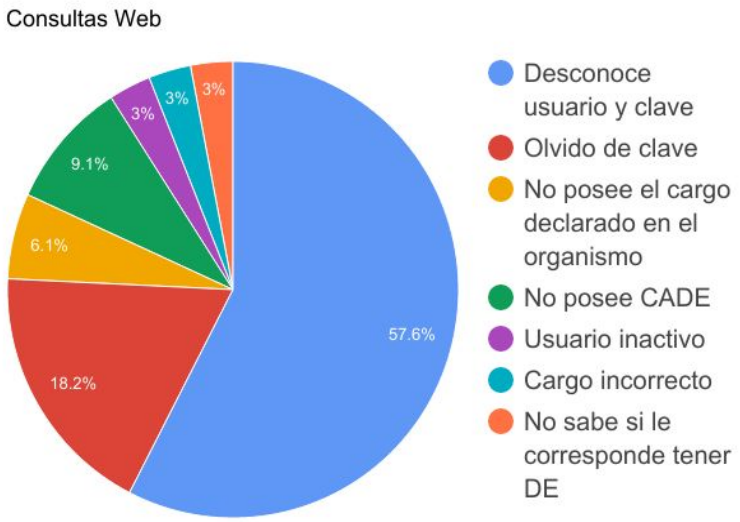
	Fallo	**Traslado 27**	**Traslado 39**	**Comunicación Simple**
Cantidad de notificaciones	261	667	66	25

Gracias a la solución implementada se ha logrado un plazo máximo de 4 días y un promedio de 30 horas para que las notificaciones sean efectuadas. Esto demuestra una mejora muy significativa con respecto a las notificaciones en papel que en promedio tardan 30 días.

Con respecto a los usuarios del organismo que firman digitalmente podemos decir que a Julio de 2017, existen 61 que poseen token y se encuentran en condiciones de firman con ***Segno***. Vale aclarar que 17 usuarios utilizan el firmador en distintas delegaciones distribuidas en la Provincia de Buenos Aires, el resto se encuentra en Sede Central.

Consultas Web - Estadisticas

De acuerdo a la información recopilada de la base de datos el día 02/03/2017 correspondiente a los últimos 5 meses, se ha podido observar las distintas consultas que han realizado los cuentadantes desde el formulario web. Dicha información puede visualizarse en el siguiente gráfico:



6.2. Conclusiones

En los últimos años la tecnología ha vivido un crecimiento exponencial, hecho que debe ser acompañado por la administración pública a los efectos de modernizar sus procesos. En este contexto, se plantea Notificación Electrónica, como un proyecto innovador y de gran impacto para los procesos principales del organismo.

En el año 2015 se planteó el concepto y creó la Comisión para llevar adelante este tema, definiéndose los componentes básicos que formaron parte del proyecto deseado, tales como: Declaración Jurada Web, Domicilio Electrónico y Firma Digital. Cada uno de ellos se fueron abordando, con continuidad y persistencia, resolviendo todas las dificultades encontradas y previendo a su vez las posibles complicaciones que podrían surgir a lo largo de cada una de las fases del proceso de desarrollo.

De manera particular se hace hincapié en el firmador digital, como el componente que representó el desafío más interesante a nivel tecnológico, ya

que no había un software que cumpliera con todos los requisitos que el organismo definió para la Firma Digital.
A lo largo de este trabajo se describieron problemas encontrados en firmadores hallados en el mercado y los respectivos argumentos que denotan por qué no se adoptaron en el HTC. Esta situación coyuntural fue un impulso para la búsqueda de una resolución adecuada en base a las fortalezas de recursos, herramientas y capacidades disponibles.
Los inconvenientes pudieron resolverse por medio de la implementación de un firmador digital propio denominado ***"Segno"***. Resulta satisfactorio como proyección personal dirigida a los usuarios, el desafío que propone el desempeño de la creatividad y la constancia en la evolución de esta tecnología. Pero también, cabe mencionar que este tipo de aplicaciones tiene una limitación, siendo la comunicación con el token el principal inconveniente.
Para lograr mayor celeridad y seguridad procesal se tuvieron en cuenta varios aspectos y modelaron distintos componentes que permitieron la correcta comunicación entre sí alcanzando los objetivos planteados desde un principio.
Uno de los objetivos focales de este trabajo fue el estudio del proceso de notificación electrónica en el ámbito público.
Actualmente, Segno es utilizado por los funcionarios del HTC para firmar digitalmente todos los documentos que son enviados a aquellos cuentadantes adheridos a participar voluntariamente en el circuito de notificación electrónica, el cual, vale aclarar, será obligatorio a partir del año 2018.
Finalizando una visión global, los beneficios que ha generado el uso de firma digital y la notificación electrónica en el HTC son notorios y apreciables, aclarando que no sería complicado implementar un proceso similar en otros organismos que requieran este tipo de soluciones.

6.3. Trabajos a futuro

Cómo trabajos a futuro se proyectan las siguientes tareas:

- Generar material de capacitación para los usuarios de *Segno* dentro del HTC y para los cuentadantes, que sirva de utilidad para comprender los principales conceptos de firma digital y su importancia dentro del ámbito público.

- Agregar nuevas aplicaciones que provean de distintos documentos y puedan ser firmados con Segno.

- Incorporar otros tipo de archivos a firmar, cómo XML o .doc.

- Incorporar la posibilidad de seleccionar el sector del documento donde se ubicará la estampa con el logo y datos del firmante.

- Mejorar el mecanismo de interacción entre Segno y las aplicaciones que se ejecutan en el servidor. Para ello se plantea “Segno IO”, el cual nace como mejora de la versión anterior (Segno) con el objetivo de mejorar la interacción con el usuario y aspectos de la seguridad en la comunicación entre los componentes. Dicha solución se encuentra en desarrollo y se espera implementar paulatinamente para todos los usuarios que actualmente usan Segno. La novedad de esta implementación es el uso de Socket.io[52] para la comunicacion entre los componentes de la solución; una tecnología basada en WebSockets, que permite manejar eventos en tiempo real y comunicaciones bidireccionales.

- Incorporar firma digital a otros procesos de la organización a partir de la experiencia de la implementación y el uso de Segno.

Referencias

[1] http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
[2] http://www.gob.gba.gov.ar/legislacion/legislacion/l-13666.html
[3] http://www.htc.gba.gov.ar
[4] http://www.htc.gba.gov.ar/resolucion-007-2015
[5] https://es.wikipedia.org/wiki/Criptograf%C3%ADa
[6] https://ibm.co/2tgq2WE
[7] https://imarrero.webs.ull.es/sctm03.v2/modulo3/PCaballero.pdf
[8] http://bit.ly/2sN6Dvm
[9] https://es.wikipedia.org/wiki/Cifrado_negable
[10]https://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales
[11] https://tools.ietf.org/html/rfc3447
[12] http://www.firmadigital.gba.gob.ar/
[13] https://es.wikipedia.org/wiki/Firma_digital#Propiedades_necesarias
[14] http://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html
[15]http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf
[16]http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.01_60/ts_101903v010401p.pdf
[17] https://www.ietf.org/rfc/rfc2315.txt
[18] https://www.w3.org/TR/xmldsig-core/
[19] https://www.ietf.org/rfc/rfc3647.txt
[20] https://www.ietf.org/rfc/rfc3280.txt
[21] https://en.wikipedia.org/wiki/Certificate_revocation_list
[22] https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol
[23] https://tools.ietf.org/html/rfc6960
[24] http://www.arcesio.net/snmp/asn1.html
[25] Yongge Wang (2012). Public Key Cryptography Standards: PKCS. http://bit.ly/2sR0k89
[26] https://tools.ietf.org/html/rfc2898
[27] https://tools.ietf.org/html/rfc3852
[28] https://www.ietf.org/rfc/rfc2986.txt
[29] https://tools.ietf.org/html/rfc7512
[30] https://tools.ietf.org/html/rfc7292
[31] Sabolansky, Alejandro Javier (2010). Utilizando software libre para un servicio de sellado digital en el tiempo. http://hdl.handle.net/10915/4025
[32] https://www.ietf.org/rfc/rfc3161.txt
[33] https://www.rfc-editor.org/rfc/rfc3628.txt
[34] Sosa, A (2009). Notificaciones procesales. Civil y comercial 2da edición. Editorial La ley.
[35] https://www.pjn.gov.ar/Publicaciones/00021/00056819.Pdf
[36] Maurino, Alberto L.(2014), “Notificaciones Procesales” 3era edición. Editorial Astrea, Bs As.
[37] Gobierno Electrónico: Gobierno, Tecnología y Reformas. Piana, Ricardo Sebastián. Edulp.2007.

[38] Marcuzzo, Inés María (2016). Firma Digital: propuesta de un sistema de notificaciones electrónicas para el Honorable Tribunal de Cuentas de la provincia de Buenos Aires. http://sedici.unlp.edu.ar/handle/10915/60133
[39]http://servicios.infoleg.gob.ar/infolegInternet/anexos/180000-184999/184193/norma.htm
[40]http://servicios.infoleg.gob.ar/infolegInternet/anexos/195000-199999/195870/norma.htm
[41]http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/221022/norma.htm
[42] http://www.htc.gba.gov.ar/images/legislacion/ConstitucionBsAs.pdf
[43] http://www.gob.gba.gov.ar/legislacion/legislacion/l-10869.html
[44] Coronel Juan Enrique, Pardo Sebastián, Groizard Mariano Ezequiel, Márquez Germán (2016). Yuran: Una herramienta informática para el fortalecimiento del Sistema de Gestión de Calidad en el Honorable Tribunal de Cuentas de la Provincia de Buenos Aires. http://45jaiio.sadio.org.ar/sites/default/files/SIE-13.PDF
[45] https://www.xolido.com/lang/xolidosign/
[46] Rodriguez, Elida Ida y Sierras, Roberto Daniel (2014). Firma digital y despapelización. *Experiencia exitosa entre ANMAT y su industria regulada.* XLIII Jornadas Argentinas de Informática e Investigación Operativa (43JAIIO)-VIII Simposio Argentino de Informática del Estado (SIE) (Buenos Aires, 2014). http://sedici.unlp.edu.ar/handle/10915/41927
[47] http://www.cren.net/crenca/onepagers/hsm2.html
[48] http://www.vmware.com/
[49] https://www.debian.org/
[50] http://httpd.apache.org/
[51] https://www.mysql.com/
[52] https://socket.io/